Research Report: Femtech Apps and Wearables and GDPR Compliance

An Empirical Study of Femtech's Privacy Policies and Terms of Service under the GDPR

Maria Tzanou, Anna Nelson, George Surtees
and Tsachi Keren-Paz

LEVERHULME TRUST

Acknowledgements 4
About the authors 4
Executive Summary 5
1. Introduction: Definitions and Purpose of the Study 10
Context: What is Femtech? 10
2. Purpose of the Report and Wider Research 11
Methodology 11
A. Selecting Apps for Study 11
B. Reviewing the Privacy Policies 15
3. Privacy Summaries 15
4. Mention of Legal Frameworks 16
5. Data Collection & Data Processing 16
Data Collected 16
6. Principles relating to the processing of personal data 19
7. Legal Basis for processing 20
Purposes of Processing 24
Processing for wider research purposes (excluding internal product development) 26
Joining the Dots: Specific Types of Data, Purposes for Processing and Legal Basis 27
8. Changes to the Privacy Policy 30
9. Processing of Children's/ Girls' Personal Data 31
10. Data Storage 34
11. Data location 36
12. Data Sharing 37
Sharing Data with Law Enforcement 38
13. Targeted Advertising 40
Opting out from targeted advertising 41
Data processed for advertising by third-parties 42
Data shared with third-parties for profit 44
14. Femtech Business Models and Their Impact on User Experience 46
Wearable-Associated Apps 47
'Women-Owned' femtech (as a Marketing Tool) 48
15. Data Subject Rights 49
16. AI Processing 51
17. Data Security 55
18. Community groups 59
19. Data Protection Impact Assessments (DPIAs) 61
20. Data Protection Officers (DPOs) 61

21. Right to Lodge a Complaint 61
22. Data Transfers 62
23. Terms of Service documents 63
Disclaimers of Warranty 68
Excluded Liability 70
Contractual Liability 71
Ownership, licensing, and monetisation of data 71
Jurisdictions 71
Distinction Between Wearable and App / Hardware and Software 72
Relationship Between The Terms of Service and The Privacy Policy 72
Conclusions 74
Recommendations 80
Femtech companies 80
Users 82
Data Protection Authorities (DPAs) 84
Policy-makers 85
Courts 87
Civil society, media and academia 88

Acknowledgements

The research for this study was generously funded by a Leverhulme Trust Research Project Grant RPG-2022-015. The research underpinning the report was undertaken by Dr Anna Nelson and subsequently by Dr George Surtees.

About the authors

Tsachi Keren-Paz is a Professor of Private Law at the University of Sheffield and the Co-Investigator of the Leverhulme Research Project Grant. His research focuses on tort law, private law theory, privacy, gendered harms, medical liability, and law and innovation.

Anna Nelson is a socio-legal researcher with a particular focus on issues of consent and care in the childbirth context. She has broader research interests in gendered experiences of health care, and reproductive technologies. She obtained her PhD in Bioethics and Medical Jurisprudence from the University of Manchester, and her doctoral research focussed on artificial womb technology and the legal protection of autonomy during childbirth, and is currently a Research Associate on the UKRI-funded ConnecteDNA Project.

George Surtees has a PhD in Philosophy from the University of Sheffield. His research focuses on feminist philosophy (particularly epistemic injustice), intellectual humility, and the philosophy of friendship, and how these areas intersect.

Maria Tzanou is a Senior Lecturer in Law at the University of Sheffield and the Principal Investigator of the Femtech Leverhulme Research Project Grant. Her research focuses on data protection, privacy, surveillance, gendered data justice and the regulation of emerging technologies.

Executive Summary

'Femtech' refers to a multi-billion-dollar technology industry that offers a variety of technological tools to monitor and manage women's sexual and reproductive health and wellbeing. It encompasses a broad range of software (apps) and hardware (wearables) aimed at supporting women and gender minorities to manage their menstrual, reproductive and sexual health. Femtech apps track a range of different aspects of women's sexual and reproductive health, such as menstruation, fertility and menopause.

Femtech **apps** purport to make predictions about future experience (i.e. fertility windows and the start date of future menstrual cycles) and to offer 'personalised' information about menstrual/reproductive health and symptom management on the basis of relevant information provided by users.

Femtech **wearable devices** are worn on or in the body and use sensors to gather information, such as breast milk production, pelvic floor muscle movements, changes to cervical fluid and basal body temperature. Using a connected app, wearables provide information or direct 'bio-feedback' to users; for example, smart pelvic floor trainers may use vibration to guide the user's exercises.

This study's understanding of femtech also encompasses **smart sex toys** designed for use by women, such as smart vibrators and smart dildos. Many smart sextech products are able to be remotely controlled (for example by partners), while some collect biometric data from the user.

This study examined the compliance of **42 femtech apps, including 15 wearable-associated apps**, with data protection law and in particular with the **European Union's (EU's) General Data Protection Regulation (GDPR)**. Compliance was assessed through an empirical analysis of the Privacy Policies and Terms and Conditions of the selected apps. The study forms part of a broader Leverhulme Trust funded research project which explores the digital gendered harms of femtech surveillance and investigates regulatory, including remedial, responses to these.

This report is followed by—and can be read in conjunction with—two further research reports carried out within the Leverhulme Trust funded research project grant: one focusing on **femtech users' reviews** analysis; and, another offering a **traffic analysis of femtech data sharing**. [1]

A number of caveats about the discussion are required. First, we recognise that not all those who menstruate, conceive and use 'femtech' are women, and that femtech may be used by people of different genders, including (but not limited to) transgender males, intersex and nonbinary persons. We note, however, that the overwhelming majority of users self-identify as women and that the femtech industry often markets exclusively to cisgender women, relying on stereotypical images of femininity when targeting this demographic. Secondly, the report does not purport to single out specific apps or wearables identifying them either as good or bad practice regarding data privacy. In this regard, it does not aim to act as a marketing tool directing users to certain apps. We recognize that a decision to use a certain app or wearable is

[1] Both research reports to be published alongside other project outputs here: https://www.sheffield.ac.uk/siccl/projects/femtech-surveillance-gendered-digital-harms-and-regulatory-approaches.

something that entails several other factors not included in the present analysis, including the apps' functionality and accuracy of predictions, its presentation, accessibility, cost (where applicable) and the purposes that users are trying to achieve, etc. Instead, the present discussion aims to provide: a) an empirical analysis of femtech Privacy Policies and Terms of Service; followed, by b) a legal assessment of their compliance with data protection law and in particular the GDPR. Based on these findings, it offers specific recommendations addressed to different interest groups and stakeholders. Thirdly, we have decided to provide a comprehensive and detailed analysis of the topics surveyed. This means that, as a result, the overall report is lengthy. To mitigate this issue, we have tried to make the discussion as reader-friendly as possible. The report can be read in its entirety or readers could use the hyperlinked Table of Contents to read specific parts or they could indeed turn to the conclusions and recommendations section which summarises the analysis and our proposals.

The present report revealed that there is a varying degree of compliance of femtech Privacy Policies with the data principles, obligations and subjects' rights under the GDPR. The main findings of the empirical analysis are:

1. Femtech Privacy Policies **vary** significantly with regard to their **clarity, level of detail** and **substantive compliance** with the GDPR.

2. This variance was observed **across apps** (comparing different apps with each other) but also **within apps** (compliance with different GDPR requirements could be differential within the same app). Indeed, the study identified several problematic areas of concern regarding femtech apps' Privacy Policies.

3. The provisions in femtech's **Terms and Conditions**, more specifically those relating to various **disclaimers** as to the functionality of the apps, data security and the liability of controllers, were very **wide** and often **diverged** from relevant statements made in the app's Privacy Policy. This might mislead users, especially those who read only the Privacy Policy.

4. Some femtech apps did not mention at all that they process **health related sensitive personal data**. Others, while acknowledging that they processed data, did not provide any differentiation regarding the relevant categories of such data, beyond broad and general qualifications, such as 'wellness' data. This is particularly problematic because it fails to identify the intimate and often embodied nature of femtech related data (and their concomitant risks and harms of their processing) as well as their gendered dimension. Specifically, there was insufficient attention to the fact that intimate wearables raise concerns about physical privacy and bodily integrity.

5. A relative minority of the apps surveyed specified **consent** as the legal basis for processing special category data under Article 9 GDPR and even fewer stated that the consent must be explicit.

6. Information about the **data sharing policies** of the apps was often convoluted or obscured behind unclear statements, such as "*We **may** share your data*" with third parties. Only a minority of the apps studied was found to comprehensively list all the third parties with whom information is shared.

7. More generally, the use of the modal verb '**may**' to describe different approaches to how personal data is processed was prevalent and questionable. The generic terminology and the ambiguous use of 'may' in the Privacy Policies can be especially confusing to users. It is widely known that users often have limited time to read Privacy Policies and uncertain wording might exacerbate this general uneasiness to engage with such documents.

8. The vast majority of apps were explicit in the fact that they **share data with law enforcement** authorities if required to do so by law. While the explicit acknowledgment is important, the sharing itself is particularly concerning as femtech data could be used to support abortion prosecution or more broadly to undermine reproductive health autonomy, especially in the current environment of surveillance of women's bodies and choices following the US' Supreme Court's decision in *Dobbs v Jackson* which overturned *Roe v Wade.* Abortion laws vary across Europe, but it is important to note that restrictions on lawful termination are in place in a number of EU countries and most notably in Poland. The research revealed that **several apps demonstrated a greater degree of appreciation** of the potential risks and harms of sharing data in this regard. A number of them indicated that they would carefully review requests to ensure there is a specific investigative purpose justifying the request existed and others stated that they would notify users before sharing any data with law enforcement. Finally, **some apps indicated a willingness to resist such requests**.

9. Many (but not all) apps stated in their Privacy Policies that they process **children**'s data. This is particularly important because femtech apps are often used by girls/ minors to track (and learn more about) menstruation, sexual and reproductive health. Apps that processed children's data included minimum age requirements, although these could be different for different jurisdictions. **None of the Privacy Policies provided information regarding additional steps they took to protect the children's data** they process. Thus, while children's data was highlighted by some of the privacy policies, it was unclear whether it was processed in a way reflecting the nature of this information and the vulnerability of children as data subjects.

10. Many privacy policies were deficient in explaining to users their rights under the GDPR, the fundamentals of the governing framework and controllers' obligations.

11. Several apps did not mention anything about the **legal basis** for processing, while others mentioned in a generic way several legal bases provided for under the GDPR without any further explanation or clarification.

12. The majority of policies made reference to some **data subject rights** under the GDPR-right of access, right to rectification, right to restriction of processing, right to data portability and right to object. However, in many cases they did not comprehensively address all the rights provided for in Chapter III of the GDPR. Some apps did not mention any data subject right.

13. There was substantial variance in approach taken by the studied apps as to the **connections** they drew between the specific **types** of data being processed, the specific processing **purpose**

or activity and the **legal basis** for the processing. Several policies drew no such direct links, or provided only limited information regarding this.

14. While some Privacy Policies provided clear **data retention** duration periods, others opted to use general, broad statements, such as that information would be kept for as long as is required to fulfil the purpose for which it was collected. This can again increase the uncertainty of users.

15. Most apps did not specify the **location** where the data was stored. This general failure to inform femtech users about location is problematic, although we recognise that this might be a complex assessment given the fact that different interconnected services work through geographically distributed servers.

16. A minority of the analysed Privacy Policies mentioned explicitly **artificial intelligence** (AI) / automated or algorithmic processing. In some cases, such a mention was brief and oblique, merely referring to a relevant machine learning platform. Our research also revealed that a number of apps made use of such tools, without mentioning this in their Privacy Policies or Terms of Service.

17. The report revealed varying degrees of **data security** compliance. Some apps' Terms of Service explicitly disclaimed data security. Sometimes these disclaimers used language that seemed to shift the burden of responsibility away from the data controller to the data subjects. Variation was also observed regarding encryption and the categories of femtech data which were encrypted.

18. Only two policies made explicit mention of data protection **impact assessments** (DPIAs), though neither provided specific details about whether these were accessible to users and how.

19. Overall, the empirical research on femtech apps' and wearables Privacy Policies and Terms and Conditions shows **significant shortcomings that concern very fundamental aspects of femtech users data handling and the sharing of highly intimate data with third parties**. The often uncertain terms used in Privacy Policies about how femtech data are processed raise serious concerns about potential **gendered harms**.

20. The study's **concluding** remarks highlight the potential implications of such **gendered harms** and call for greater transparency, certainty and clarity in the way femtech's Privacy Policies are framed as well as the way femtech controllers demonstrate compliance with their relevant data protection legal obligations under the GDPR. The study also highlights the disregard of controllers to the fact that **wearables raise concerns regarding physical privacy and bodily integrity – not only informational privacy**.

21. The report provides a number of **Recommendations**. These are addressed to femtech industry actors/ controllers, to users, to regulators (DPAs), to policy-makers, to courts and to civil society, media and academia.

1. Introduction: Definitions and Purpose of the Study

Context: What is Femtech?

The term 'Femtech' was coined by Ida Tin, the co-founder of menstrual tracking app Clue. 'Femtech' encompasses a broad range of software (apps) and hardware (wearables) aimed at supporting women and gender minorities to track, understand and manage their menstrual, reproductive and sexual health. Femtech promises to empower women to achieve a 'quantified' knowledge of the 'self' and to redress the balance following centuries of androcentric medicine. Femtech apps operate on the basis of data the user inputs directly. Some apps are designed specifically to operate in conjunction with a particular 'wearable' – these are devices which are worn in or on the body which use sensors to gather biometric information, such as body temperature, menstrual flow or heart rate. These apps can combine data from the wearable with additional data inputted by the user.

To understand the use and popularity of femtech apps and devices, it is necessary to situate these within the broader social and medical context within which they exist (and were developed). There is a recognised tendency to question whether women are trustworthy narrators of their own health and pain,[2] particularly regarding conditions related to the (dis)functioning of the womb.[3] Those experiencing gynaecological symptoms are often 'not listened to'[4] and can face a 'battle' for diagnosis and treatment.[5] There are also substantial knowledge gaps regarding the ways that different gynaecological conditions manifest,[6] as women's health remains under-researched. Sexual, obstetric, post-partum and gynaecological health services are often under-resourced and subject to austerity measures,[7] struggling to meet patients' needs within an appropriate time frame or with satisfactory quality.[8]

---

[2] Anna Nelson, 'Medical Records and Epistemic Injustice: A Women's Health Issue Worthy of Greater Attention' (*APA Blog*, 11 Sept 2023). Available at: www.blog.apaonline.org/2023/09/11/medical-records-and-epistemic-injustice-a-womens-health-issue-worthy-of-greater-attention/.

[3] See, eg, Stella Villarmea, 'When a Uterus Enters the Room, Reason Goes out the Window' in C Pickles and J Herring (eds), *Women's Birthing Bodies and the Law: Unauthorised Intimate Examinations, Power and Vulnerability* (Hart 2020), 70–73; Elinor Cleghorn, *Unwell Women: A Journey Through Medicine And Myth in a Man-Made World* (Weidenfield and Nicolson 2021).

[4] Department for Health and Social Care, *Women's Health Strategy for England* (CP736, Her Majesty's Stationery Office 2022), 7.

[5] All Party Parliamentary Group on Endometriosis 'Inquiry Report; Endometriosis in the UK: Time for Change' (2020) 27.

[6] It was reported recently that have some women have switched to femtech apps after struggling on hormonal treatments like the pill. Michelle Roberts and Rozina Sini, '"Pregnancy is a risk I'm willing to take": Why some women are ditching the pill', BBC News, 18.01.2025 https://www.bbc.co.uk/news/articles/c93lq2w5n44o.

[7] Daniela Alaattinoğlu, 'Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps' (2022) 30 *Feminist Legal Studies* 157, 161.

[8] For example, in its 2022 report, the UK Royal College of Obstetricians and Gynaecologists noted that more than half a million women (570,000) were on waiting lists for gynaecological appointments across the UK, and that more than one in 20 patients in England had to wait more than a year for treatment – often for conditions such as endometriosis which have debilitating symptoms. See D Khanna, 'Women's health: Why is the health of at least half the global population so often overlooked?' (*World Economic Forum*, 2 Jan 2022). Available at:

Against this backdrop, women often feel that they have to turn to femtech to fill the gaps left by traditional healthcare services. This also means that femtech products—especially wearables—should be potentially evaluated not only from an informational data perspective but also from a health care perspective and that they raise concerns about gendered harms, patients' autonomy (when both 'patient' and 'health care' are broadly defined) and, in cases of wearables, also bodily integrity and physical privacy.[9] While the current state of women's healthcare operates as a 'push' factor in the femtech context, the marketing of femtech apps and wearables provides a complimentary 'pull' factor. Much of this marketing centres upon a promise to 'empower' women and gender diverse users with knowledge about their own sexual and reproductive health, a promise which may resonate well in light of the frustrating lack of appropriate healthcare.[10]

2. Purpose of the Report and Wider Research

The aim of this report is to assess the extent to which femtech apps (including wearable-associated apps) comply with the provisions of the EU's General Data Protection Regulation (GDPR).[11] The report forms part of a wider Leverhulme Trust funded research project which interrogates regulatory, including remedial, responses to femtech surveillance, and explores whether these adequately reflect and address the potential harms associated with femtech.[12]

Methodology

A. Selecting Apps for Study

Total apps included: 42

App only: 27

App associated with a wearable: 15

We first identified the primary categories of femtech app and wearable devices using marketing insights,[13] and a non-systematic approximation of saturation sampling searches of the Google

www.weforum.org/agenda/2023/01/women-health-gap-davos-2023/; L Hoctor et al, 'Women's sexual and reproductive health and rights in Europe: Issue Paper' (*Council of Europe Commissioner for Human Rights,* December 2017); Royal College of Obstetricians & Gynaecology, 'Left for too long: understanding the scale and impact of gynaecology waiting lists'. Available at: www.rcog.shorthandstories.com/lefttoolong/index.html; Elvie and Motherly, *The Motherload - The Weight of Limited Postpartum Support* (2024).

[9] Tsachi Keren-Paz, Anna Nelson and Maria Tzanou, 'Femtech wearables and embodied harm: a new regulatory approach' (under review, 2025).

[10] NIHR Evidence, 'Women's Health: Why do Women Feel Unheard?' (Health and Social Care Research, 23 November 2023).

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (GDPR) [2016] OJ L119/1.

[12] For more information on the project's outputs, see https://www.sheffield.ac.uk/siccl/projects/femtech-surveillance-gendered-digital-harms-and-regulatory-approaches.

[13] Including statistics generated by Statista (https://www.statista.com/) regarding leading period tracker and female health apps by both downloads and revenue: data collected as of September 2023.

Play Store and media articles (until no new categories of app / app + wearable were being identified in each search).

Using this approach we identified eleven primary app-only categories of interest: (1) Fertility Tracker, (2) Ovulation Tracker, (3) Menstrual Tracker, (4) Menstrual Condition Tracker (e.g. PMDD), (5) Menopause Tracker, (6) Pregnancy Tracker, (7) Foetal Movement Tracker, (8) Contraction Tracker & Timer, (9) Breastfeeding Tracker, (10) Breast Health Tracker and (11) Mood Tracker.[14]

We also identified six primary categories of wearable-associated app: (1) Fertility Tracker,[15] (2) Breast Pump, (3) Pelvic Floor Trainer, (4) Health & Activity Tracker with a Menstrual Tracking Feature, (5) Menopause Symptom Tracker / Relief and (6) SexTech (e.g. smart vibrator).

As our interest is in femtech products that entail women's self-tracking and management of their sexual and reproductive health and wellbeing, we excluded femtech which falls into the following categories: (1) Telehealth, (2) Clinical Tools, (3) Supplements and Nutrition and (4) Speculative Technologies.

We then inputted each category into the Google Play Store,[16] with results being ordered according to the Play Store ranking.[17] For each category we included the most downloaded app, and any additional apps which had over ten million downloads. We then checked these results for duplicate (apps falling in multiple categories) and removed these. At a second stage, we cross checked our results against market reports & the Apple App Store in order to ensure that we did not miss any important apps out. We then included in our sample any apps / wearable-associated not identified in the initial search, which met one of the three additional criteria:

1. Any femtech apps recommended **by the NHS or by UNICEF or the WHO**, as long as these were available in English and on the UK android App Store. Where there is a

[14] We note that there is substantial overlap with these categories, and many of the apps offer services across multiple categories.
[15] Fertility tracking wearables deploy three different measuring methods: measuring basal body temperature, measuring cervical mucus and measuring a combination of basal body temperature, and progesterone.
[16] We selected Google Play Store as the relevant app marketplace for practical reasons, to allow us to link the legal analysis to the computer science analysis which was also undertaken as part of this project.
[17] "*Google Play search factors in the overall experience of your app based on user behaviour and feedback. Apps are ranked based on a combination of ratings, reviews, downloads and other factors…. the details of these weights and values are a proprietary part of the Google search algorithm"* - Get discovered on Google Play search - Play Console Help

'medical push' towards using a particular app or wearable, we considered it particularly important to study the relevant privacy policy[18] (Oky,[19] Elvie Trainer[20]).

2. Any apps which were connected to **significant news stories about privacy** (breaches and beyond) (FEMM,[21] Glow,[22] Ovia: Fertility, Cycle, Health,[23] Ovia: Pregnancy & Baby Tracker).[24]
3. Any apps which are **not-for-profit:** there is often a perception that privacy and profit are in tension in the femtech realm, so we were interested to see whether non-for-profit apps had compliant data privacy practices (Drip, Euki, Spot-On).

For practical and feasibility reasons, we required that the apps be available (1) in English, (2) for Android and (3) on the UK Google Play Store.

The table below lists all the apps which were included in the research which informs this Report:

App Name	App Only or Wearable-Associated App	Head-Quarter Location
Clover - Safe Period Tracker	App only	Cyprus
Clue period tracker & calendar	App only	Germany
FEMM Health and Period Tracker	App only	USA (New York)
Flo Period & Ovulation Tracker	App only	Incorporated: USA (Delaware) Global Headquarters: UK (England)
Frendo Endometriosis Tracker	App only	Ireland

[18] Anna Nelson, Maria Tzanou & Tsachi Keren-Paz, 'Recommending Privately-Developed FemTech in Healthcare Part 1: Promises and Pitfalls' (BMJ SRH, 16 Sept 2024) <https://blogs.bmj.com/bmjsrh/2024/09/16/femtech-part-1/> accessed: 14 October 2024; Anna Nelson, Maria Tzanou & Tsachi Keren-Paz, 'Recommending Privately Developed FemTech in Healthcare Part 2: Understanding Healthcare Professionals' Responsibilities' (BMJ SRH, 3 Oct 2024) <https://blogs.bmj.com/bmjsrh/2024/10/03/recommending-femtech-part-2/> accessed: 14 October 2024.

[19] Alexandra Tyers, 'Oky: Co-created with girls, for girls' (*UNICEF*, 28 April 2020) <https://www.unicef.org/innovation/stories/oky-co-created-girls-girls> accessed: 20 August 2024.

[20] Elvie, 'Elvie and the NHS' <https://www.elvie.com/en-gb/elvie-and-the-nhs> accessed: 20 August 2024.

[21] Jessica Glenza, 'Revealed: women's fertility app is funded by anti-abortion campaigners' (Guardian, 30 May 2019) <https://www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners> Accessed: 20 August 2024.

[22] 'Fertility Tracking App Glow Exposes 25 Million Users in Data Breach' (Enterprise Security Tech, 14 February 2024) < https://www.enterprisesecuritytech.com/post/fertility-app-glow-exposes-25-million-users-data-breach> Accessed 30 January 2025

[23] Drew Harwell 'Is your pregnancy app sharing your intimate data with your boss?' Washington Post, 10 April 2019) <https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/> Accessed: 20 August 2024.

[24] Ibid.

Glow Cycle & Fertility Tracker	App only	USA (California)
Healofy Pregnancy & Parenting	App only	India (Bangalore)
Health & Her Menopause App	App only	UK (Wales)
Kindara Fertility & Ovulation	App only	USA (Colorado)
Know Your Lemons - Self Exam	App only	USA (Idaho)
Me v PMDD	App only	USA (Florida)
MenoLife - Menopause Tracker	App only	USA
Moody Month: Cycle Tracker	App only	UK (England)
My Calendar - Period Tracker	App only	USA (Washington)
Natural Cycles - Birth Control	App only	Sweden
Oky Period Tracker App	App only	USA (New York)
Ovia: Fertility, Cycle, Health[25]	App only	USA (Massachusetts)
Ovia: Pregnancy & Baby Tracker	App only	USA (Massachusetts)
Ovulation & Period Tracker	App only	Singapore
Ovy Partner - Share your Cycle	App only	Germany
PCOS Tracker	App only	USA (New York)
Period Calendar Period Tracker	App only	Hong Kong
Pregnancy + | Tracker App	App only	UK
Pregnancy App & Baby Tracker	App only	USA
Pregnancy Tracker: amma	App only	Hong Kong
SpotOn	App only	USA (New York)
Stardust	App only	USA (New York)
Elvie Trainer	Wearable-associated app	UK
Pump with Elvie	Wearable-associated app	UK
Embr Wave 2: Hot Flash Relief	Wearable-associated app	USA (Massachusetts)
Femometer - Fertility Tracker	Wearable-associated app	Hong Kong
Garmin Connect™	Wearable-associated app	Operational Headquarters: USA
Kegg	Wearable-associated app	USA (California)
Lioness Health	Wearable-associated app	USA (California)
Lovense Remote	Wearable-associated app	Singapore
Medela Family - Breast Feeding	Wearable-associated app	UK
Oura	Wearable-associated app	Finland
OvuSense	Wearable-associated app	UK
Ovy	Wearable-associated app	Germany (Hamburg)

[25] The Ovia: Fertility, Cycle, Health app was included in the research, because it came up when searching in the UK Google Play Store. However, when it came to actually attempting to download this app in order to conduct further research we were informed that "this is not available to download in your country".

Tempdrop	Wearable-associated app	Israel
We-Vibe	Wearable-associated app	Canada (Ontario)
WHOOP	Wearable-associated app	USA (Massachusetts)

B. Reviewing the Privacy Policies

Once the apps had been selected, the project team developed a 'codebook' containing the information we sought to identify in each policy.[26]

The Privacy Policy (sometimes called Privacy Notice) and Terms & Conditions (sometimes called Terms of Use or Terms of Service) were reviewed for each of the selected apps. A copy of these documents as correct at time of analysis (between February and April 2024) was downloaded and saved. We recognise that both Privacy Policies and Terms and Conditions may be edited or updated in the future, but the present research focuses on the versions collected in the above time period.

3. Privacy Summaries

We note that there is significant variation in the length of Privacy Policies (these range from 3 to 49 pages).[27]

In addition to the main privacy policy, some of the apps provided a short / readable summary of the key points, either at the start of the main document or in a separate location. In some cases these summaries made explicit that users should read the main policy (Flo: *"It is not a substitute for reading the full policy, along with our Terms of Use"*), while others suggested doing so in order to access more information *if desired* (WHOOP: *"You can find more detailed information about the ways in which we use, collect, and share personal data in our full privacy policy"*).[28]

The inclusion of such summaries enhances accessibility and transparency - making it clearer and easier for the user to identify how their data will be used, if it will be shared and who it will be shared with (as the main policies can be fairly long and dense and users may either struggle to read them in detail, or not have time to do so). However, there is a chance that the practice may actually undermine transparency - providing companies a chance to highlight their positive practices while burying some of the more problematic aspects in the full policy (which, arguably, users are often less likely to read if they have the option of accessing a more concise summary).

[26] Available upon request.
[27] We do not give a detailed breakdown as differences in formatting and font size make it hard to do so with appropriate accuracy.
[28] WHOOP, 'Privacy Principles' <https://www.whoop.com/us/en/privacy-principles/> accessed 26th September 2024.

4. Mention of Legal Frameworks

The table below sets out the key legal frameworks mentioned by the apps in their policies.

	No. of Apps	Apps
GDPR mentioned in either Privacy Policy or Terms of Service	**27**	Clover - Safe Period Tracker; Clue period tracker & calendar; Flo Period & Ovulation Tracker; Frendo Endometriosis Tracker; Glow Cycle & Fertility Tracker; Health & Her Menopause App; MenoLife - Menopause Tracker; Moody Month: Cycle Tracker; My Calendar - Period Tracker; Natural Cycles - Birth Control; Ovulation & Period Tracker; Ovy Partner - Share your Cycle; Period Calendar Period Tracker; Pregnancy App & Baby Tracker; Pregnancy Tracker: amma; Stardust; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Garmin Connect™; Lovense Remote; Oura; Ovy BBT; Tempdrop; We-Vibe; WHOOP
UK GDPR specifically mentioned[29]	**6**	Embr Wave 2 - Hot Flash Relief, Frendo, Glow; Moody Month, Pregnancy App & Baby Tracker, We-Vibe
Other Legal Frameworks mentioned (either by specific regulatory instrument or by jurisdiction)[30]	**24**	Flo Period & Ovulation Tracker; Glow Cycle & Fertility Tracker; Healofy Pregnancy & Parenting; MenoLife - Menopause Tracker; My Calendar - Period Tracker; Natural Cycles - Birth Control; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy & Baby Tracker; Ovulation & Period Tracker; PCOS Tracker; Period Calendar Period Tracker; Pregnancy App & Baby Tracker; Pregnancy Tracker: amma; SpotOn; Stardust; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Garmin Connect™; Kegg; Lovense Remote; Medela Family - Breast Feeding; Oura; OvuSense; WHOOP

It should be noted that simply mentioning the GDPR does not necessarily indicate substantive compliance with this law. Further assessment of the policies is needed to ascertain this.[31]

5. Data Collection & Data Processing

Data Collected

Personal Data / Information: Three apps, Euki, Drip and Periodical, mentioned that they did not collect or process personal data, and that they stored all menstrual data locally on the users' device in a non-identifiable manner which cannot be linked to a natural person (the user). For example, Euki mentioned that "*Data you track in the app is not tied to your email address or*

[29] This is not limited to apps which are headquartered in the UK; Embr Wave 2 - Hot Flash Relief (USA), Frendo (Ireland), Glow (USA), Moody Month (UK), Pregnancy App & Baby Tracker (USA), We-Vibe (Canada)

[30] E.g. California Consumer Privacy Act of 2018, California Civil Code Section 1798.83, Colorado Privacy Act, the Virginia Consumer Data Protection Act, Brazilian Lei Geral de Proteção de Dados.

[31] A number of the apps (including MenoLife and Ovulation & Period Tracker) only specifically mention the GDPR when listing the data subject rights (and do not mention this explicitly anywhere else).

phone number, and only you have access to it." Such privacy by design techniques are welcome; if no personal data is processed, the GDPR is not applicable in principle.

The rest of the apps included in this report process personal data. Specific apps include versions that allow the user to not have their personal data processed.[32] For instance, Flo and Natural Cycles[33] do not process personally identifiable information when anonymous mode is activated.[34]

There was significant variation on how privacy policies identify the categories of personal data they process, with some apps providing this in detail while others mentioning broad and generic categories of data without any further clarifications (e.g., 'health data', 'wellness data').

Health, Menstruation, Reproductive and Sexual Data: 35 of 42 policies specifically mentioned the processing of health, menstrual or sexual data. These include, among others, cycle information (e.g. period length, pain, other symptoms such as spotting, etc.), body temperature, hair quality, sexual intercourse. Health–related data may be entered manually by the users, or imported into the app from third parties or other devices (such as data on sports activities, weight, calories, heartbeat rate, number of steps from Apple Health, Google Fit, fitness trackers).

Medela noted that the user may choose to input data about contractions during labour - which could be considered health data. Additionally, the Lovense Remote Policy stated that "*Audio, electronic, visual, thermal, olfactory, or similar information*" is collected. This is also personal data to the extent they are linked to an identifiable natural person.

Furthermore, Clover mentioned that it collects health-related data of unregistered users: "*When you use the App, you may choose to provide personal information about your or your child's health such as weight, body temperature, menstrual cycle dates, symptoms, health* goals, *other information about your health and activities."*

Some Policies used the terminology "well-being data" or "wellness data". For example, WHOOP referred to "wellness data" as data such as resting heart rate, heart rate variability, skin temperature, blood oxygen saturation level and acceleration; metadata on workouts and sleep; the type of physical activity the user engages in and the duration of the activity; data reflecting the strain and recovery; fitness/athlete level (e.g., professional or recreational); information about diet, medications, and female health tracking.

---

[32] Natural Cycles' Privacy policy states: "you also have the option to Go Anonymous if you need an extra layer of protection for your identity, for example, if your data is at an increased risk. If you Go Anonymous, your personal identifying information will be separated from your fertility data, which means that no one — not even us at Natural Cycles — can link your NC° data to you." See https://help.naturalcycles.com/hc/en-us/articles/20116990594333-What-is-Go-Anonymous#:~:text=If%20you%20Go%20Anonymous%2C%20your,My%20account%20and%20Settings%20pages.

[33] Natural Cycles' Privacy policy states: "you also have the option to Go Anonymous if you need an extra layer of protection for your identity, for example, if your data is at an increased risk. If you Go Anonymous, your personal identifying information will be separated from your fertility data, which means that no one — not even us at Natural Cycles — can link your NC° data to you." See https://help.naturalcycles.com/hc/en-us/articles/20116990594333-What-is-Go-Anonymous#:~:text=If%20you%20Go%20Anonymous%2C%20your,My%20account%20and%20Settings%20pages.

[34] This feature seems to have been introduced post-*Dobbs*: https://www.theverge.com/2022/9/14/23351957/flo-period-tracker-privacy-anonymous-mode. *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 (2022) overturned *Roe v Wade* 410 U.S. 113 (1973) and denied American women a privacy-based constitutional right to abortion.

According to FEMOMETER's Privacy Policy, "information regarding health and wellbeing" includes different categories of data from "menstrual cycle dates, fertility test results & images of fertility tests, including ovulation, pregnancy and progesterone", "Basal Body Temperature (BBT) readings and information", "average period length, user-recorded ovulation day, cervical mucus quality, cycle length, symptoms, menstrual flow, moods", "pregnancy status, information about foetal movement, information about insemination", "sexual behaviour, assisted reproductive technology application, cervical position", to "medication information, including name, type, and daily intake, vitamins and supplements, including name, type, and daily intake", and "health related documents and records, such as ultrasound records, blood tests, IUI sperm prep, semen analysis, LH tests, HCG tests, PDG tests, Fern tests, other fertility test results, and other test results, diagnosis, or treatment reports." Flo defined wellbeing data as personal data users provide directly, including among others "weight; height; body mass index (BMI, a value derived from the mass and height of a person), symptoms related to users' menstrual cycle, menopause, pregnancy, general well-being and health; information relating to sex life; or other information, like users' physical and mental well-being".

Location Data: 33 of 42 of the privacy policies specified that they collect some form of location data.[35] Only 5 (FEMM Health and Period Tracker, Moody Month: Cycle Tracker, Garmin Connect™, Kegg, Oura) explicitly stated that users needed to provide opt-in consent/grant specific access before such data was collected.

35 policies explicitly mentioned that IP address data was collected (either by the app provider or a third party such as Google Analytics), while 6 made no mention of this. Only one - Stardust - specifically excluded the collection of this data. Clue specified that it collected IP addresses provided by users' browsers or mobile devices, in order to deliver the service to the users' device and to determine users' approximate location for statistical and analytics purposes, and for regulatory compliance in different countries. They clarified that they 'do not collect users' precise location.

Location data has significant implications in the context of femtech as it could be used for law enforcement purposes, particularly in jurisdictions where abortion is criminalised. It is also valuable for marketing and big data processing purposes as it might help assess the socio demographic and economic profile of users.

Usage data: This includes device data (device model, name and identifiers, device settings, application identifier, crash information), information about the users' browser (browser settings, operating system, system settings). This was associated in Privacy Policies with understanding and resolving potential functionality issues.

Account data: This includes data such as a username, date of birth and email address.

It should be noted that in the femtech context device information or patterns of app use could act as proxies to sensitive, intimate information.

Some Privacy Policies provided information on the categories of sources they use to collect personal data. For instance, Ovia+ listed employers, employer health plans, health insurers and providers as its customers who might share personal data, such as employee ID numbers with

[35] Medela Family - Breast Feeding has not been included in this number, as while it requires Android users to allow access to the location (GPS) of the device in order to facilitate connection to the smart breast pump, it neither stores nor uses that data "at any time".

the app. Ovia+ also included among its data sources social networks and social media ("*If you download an Ovia app after clicking on an ad, we collect device information to show how you found Ovia*") surveys and promotions, friends referrals and lists purchases.

6. Principles relating to the processing of personal data

The research found discrepancies in the way the surveyed apps referred to different data protection principles, such as purpose limitation, data minimisation and accuracy.

Some policies specifically mentioned that data collected could be processed for further purposes. For example, Glow stated that if the "*relevant further use is compatible with the initial purpose for which the personal information was collected*" then the "original legal basis" will be relied upon, but if not separate consent will be obtained. The policy also noted that personal information may be used for "new purposes" that are "*not described in this Privacy Policy" where this is "permitted by law and the reason is compatible with the purpose for which we collected it. If we need to use your personal information for an unrelated purpose, we will notify you and explain the applicable legal basis*." Flo mentioned the purpose limitation principle ("*We will not process personal data in a way that is incompatible with the purposes for which it has been collected or authorized by you or collect any personal data that is not needed for the mentioned purposes*.")

MenoLife provided that:

> *"We may use your personal information to allow the operational functioning of this Application and features thereof ("business purposes"). In such cases, your personal information will be processed in a fashion necessary and proportionate to the business purpose for which it was collected, and strictly within the limits of compatible operational purposes…We won't process your information for unexpected purposes, or for purposes incompatible with the purposes originally disclosed, without your consent."*[36]

Certain policies mentioned the principle of data minimisation. For example, Stardust stated that they *"undertake to collect only such amount and type of Personal Data that is strictly required for the purposes mentioned…in the Privacy Policy"*[37] and Clue that their *"products and services have been designed to collect only the data necessary to provide our services. We only collect and process your data for the purposes outlined… and detailed in this Privacy Policy."*[38]

Regarding the accuracy of user data, most apps did not make clear what they did to ensure user data remained accurate[39]. When accuracy was discussed, this was in the context of the user's GDPR right to have inaccurate data corrected, but there was no information provided as to what steps the company took to maintain accuracy themselves. One exception to this

[36] MenoLife Privacy Policy.
[37] Stardust privacy policy.
[38] Clue privacy policy.
[39] It is noteworthy that accuracy is mentioned far more in the terms of service documents, with these usually stating that the company cannot guarantee the accuracy of the apps predictions and, as such, cannot be liable for the results of users acting on these predictions.

was Stardust: "*To the extent necessary for those purposes, we will take all reasonable steps to ensure that Personal Data is reliable for its intended use, accurate, complete, and current*."[40] Another was Pregnancy App and Baby Tracker:

> *"We take every reasonable step to ensure that your User Information is kept accurate and up-to-date and are erased or rectified if we become aware of inaccuracies. We take every reasonable step to ensure that your User Information that we Process is accurate and, where necessary, kept up to date, and any of your User Information that we Process that you inform us is inaccurate (having regard to the purposes for which they are Processed) is erased or rectified."*

Notably, Lovense referenced accuracy in the context of denying that the company would be at fault for inaccurate data held about users: "*You should understand, however, that information about you in our database might come from a number of sources, so any inaccuracy is not necessarily the fault of the Company*."[41]

It is interesting that the data minimisation principle was often contrasted with a need to offer accurate algorithmic predictions (or to increase their accuracy). For example, one policy stated: "*We use intelligent algorithms that provide certain App functions, such as predictions of your cycle and ovulation day. The more Personal Data about your cycle, ovulation tests, and BBT that our intelligence algorithm can work with, the better predictions you get from the algorithm.*"[42] Other apps also used accuracy as a reason for collecting personal data: "*When you use Flo, we collect your personal data and use it to improve your experience and service. We can then increase the safety and accuracy of your predictions and give you relevant app content and product offers*."[43] Likewise, Ovulation and Period Tracker stated "*The information we collect depends on how you use our services. To use the core features of our app, you may need to provide certain information, such as the dates of your recent menstrual cycle. This information will help you track your menstrual cycle more accurately to predict the timing of your next period*."[44]

7. Legal Basis for processing

29 apps mentioned one or more legal bases provided under the GDPR[45] for processing personal data, while 13 did not mention these at all. In some cases the policies set out clearly which legal basis is used for which purpose of processing (e.g. Flo, Health & Her and Natural Cycles).

Other policies merely provided a general statement which listed multiple legal bases. For example, Moody Month stated:

[40] Stardust privacy policy.
[41] Lovense privacy policy.
[42] Femometer privacy policy.
[43] Flo privacy policy.
[44] Ovulation and Period Tracker.
[45] Art. 6 GDPR.

"We use your personal data pursuant to one or more of the following legal bases as prescribed by Data Protection Legislation :

1. *to enable us to provide you with access to the MOODY App and the Services, in accordance with the agreement between you and us (as set out in our Terms of Use);*
2. *to comply with a legal obligation and/or*
3. *where it is in our legitimate interest to do so and we have indicated to you what that interest is.*"

The table below lays down information about how many Privacy Policies explicitly mentioned legal bases for processing provided in Article 6 GDPR.

Legal Basis	**No. of Policies**	**List of Apps**
Art 6(1)(a): the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;	29	Clue period tracker & calendar; Flo Period & Ovulation Tracker; Frendo Endometriosis Tracker; Glow Cycle & Fertility Tracker; Health & Her Menopause App; MenoLife - Menopause Tracker; Moody Month: Cycle Tracker; My Calendar - Period Tracker; Natural Cycles - Birth Control; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy & Baby Tracker; Ovy Partner - Share your Cycle; Period Calendar Period Tracker; Pregnancy + | Tracker App; Pregnancy App & Baby Tracker; Pregnancy Tracker: amma; SpotOn; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Garmin Connect™; Lovense Remote; Medela Family - Breast Feeding; Oura; Ovy; Tempdrop; We-Vibe; WHOOP
Art 6(1)(b): processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	26	Clue period tracker & calendar; Flo Period & Ovulation Tracker; Frendo Endometriosis Tracker; Glow Cycle & Fertility Tracker; Health & Her Menopause App; MenoLife - Menopause Tracker; Moody Month: Cycle Tracker; My Calendar - Period Tracker; Natural Cycles - Birth Control; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy & Baby Tracker; Ovy Partner - Share your Cycle; Period Calendar Period Tracker; Pregnancy + | Tracker App; Pregnancy App & Baby Tracker; SpotOn; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Garmin Connect™; Oura; Ovy; Tempdrop; We-Vibe; WHOOP
Art 6(1)(c): processing is necessary for **compliance with a legal obligation** to which the controller is subject	21	Flo Period & Ovulation Tracker; Frendo Endometriosis Tracker; Glow Cycle & Fertility Tracker; Health & Her Menopause App; MenoLife - Menopause Tracker; Moody Month: Cycle Tracker; Natural Cycles - Birth Control; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy & Baby Tracker; Ovy Partner - Share your Cycle; Period Calendar Period Tracker; Pregnancy + | Tracker App; Pregnancy App & Baby Tracker; SpotOn; Elvie Trainer; Pump with Elvie; Femometer - Fertility Tracker; Oura;Ovy;Tempdrop;WHOOP
Art 6(1)(d): processing is necessary in order to protect the **vital interests** of the **data subject** or of **another natural person**	3	Pregnancy App & Baby Tracker;[46] Period Calendar Period Tracker; WHOOP
Art 6(1)(e): processing is necessary for the performance of a task carried out	4	MenoLife - Menopause Tracker; Moody Month: Cycle Tracker; Period Calendar Period Tracker; WHOOP

[46] Pregnancy App and Baby Tracker includes a statement, which makes reference to protecting the child: "We may also disclose your User Information to prevent or address emergencies, harm, threatened harm, violence, or abuse. For example, we may disclose user information to report apparent ongoing or imminent child abuse or an imminent threat of suicide or self-harm."

in the **public interest** or in the exercise of official authority vested in the controller;		
Art 6(1)(f): processing is necessary for the purposes of the **legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	20	Clue period tracker & calendar; Flo Period & Ovulation Tracker; Frendo Endometriosis Tracker; Glow Cycle & Fertility Tracker; Health & Her Menopause App; MenoLife - Menopause Tracker; Natural Cycles - Birth Control; Ovy Partner - Share your Cycle; Period Calendar Period Tracker; Pregnancy + | Tracker App; Pregnancy App & Baby Tracker; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Garmin Connect™; Oura; Ovy; Tempdrop; WHOOP

When considering compliance with the GDPR, it is useful to explore the way that the policies engage with some of these legal bases in more detail:

Consent/ Explicit Consent: The GDPR contains specific rules for processing special category data, imposing a *prima facie* prohibition of processing thereof (Art 9(1) GDPR). Special category data, also referred to as sensitive personal data, is defined as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". Art 9(2) sets out some exceptions in which processing will be allowed. These include the data subject's explicit consent.

Of the 42 policies surveyed, 11 specified the legal basis for processing sensitive / special category data as consent.[47] Of these, 9 specified that the consent must be explicit - or 'express'.[48] Two apps recognised that there may be specific requirements to lawfully process special category data, but did not specify the particular legal basis upon which they carry out such processing. For instance:

- **Frendo Endometriosis Tracker**: *"We may collect special personal information about you if there is a lawful basis on which to do so."*

- **Pregnancy Tracker - Amma**: *"we do our best to comply with all the applicable regulations in respect to the data that we process, including any specific requirements regarding sensitive type of data in given jurisdictions. This means that if your country has higher standards of processing and protecting the sensitive data then your country's requirements will apply to your data."*

Public Interest: The policies which mentioned processing data on the basis of 'public interest'

[47] Clue period tracker & calendar; Glow Cycle & Fertility Tracker; Health & Her Menopause App; Moody Month: Cycle Tracker; Natural Cycles - Birth Control; Pregnancy + | Tracker App; Pregnancy App & Baby Tracker; Garmin Connect™; Medela Family - Breast Feeding; Oura; WHOOP.
[48] Health and Her.

or ‘in the exercise of official authority’ did not provide details or examples of the nature of that public interest. They simply included broad, non-specific statements, such as “*if it is necessary for a task carried out in the public interest”* (WHOOP).

In addition to the four apps which specifically included public interest as a legal basis for processing two (Ovia: Fertility, Cycle, Health and Ovia: Pregnancy & Baby Tracker), specified that data may be processed for “The performance…of public health activities” without further specifying what these entail.

Legal Obligations: The policies were generally non-specific regarding *which* legal obligation the data processing would fulfil. For example, Flo’s policy stated: “*Legal obligation: We may be obligated to process some of your personal data to comply with applicable laws and regulations.”* Where details were given, these tended to relate to law enforcement: “*For example, we may be required to give information to legal authorities if they so request or if they have the proper authorisation such as a search warrant or court order. This may include your personal information.*” (Frendo).

Legitimate Interests: Many of the policies included a broad, generic statement that processing is in line with the companies “legitimate interests” without specifying the particular nature of these interests. However some, such as Pump with Elvie and Elvie Trainer provided a more detailed account, specifying the particular ‘legitimate interests’ fulfilled through the processing of different types of data.

Legitimate interests included among others *“the detection and prevention of fraud*”, “*administering and improving the site*”, responding to user *“queries, support requests or complaints*”, understanding, customizing and improving *“products and services*”, dealing with any product or service errors, “*developing new products and services*", and “*tailoring*” the apps to the user.

A few policies went into more detail about how and when legitimate interests would be considered a reasonable basis for processing. The Embr Wave 2: Hot Flash Relief Policy, for example, was notable in its explicit recognition of the balancing act that underpins the use of personal data on the basis of legitimate interests:

“When we process your Personal Information for our legitimate interests, we make sure to consider and balance any potential impact on you, and your rights under data protection laws. Our legitimate business interests do not automatically override your interests – we will not use your Personal Information for activities where our interests are overridden by the impact on you, unless we have your consent or those activities are otherwise required or permitted to by law.”

Similarly, the Frendo policy specified that when data is processed on the basis of legitimate interests this is done following “careful consideration” as to (1) “*whether the same objective could be achieved through other means*”, (2) “*whether processing (or not processing) might*

cause you harm", (3) "*whether you would expect us to process your data, and whether you would, in the round, consider it reasonable to do so*."

Purposes of Processing

The apps identified a range of purposes for which they process users' data. Some policies provided specific details about exactly what types of data were processed for which specific purposes, while others merely provided a general list of purposes for which data may be processed. One policy (PCOS Tracker) omitted this information entirely.

Examples of the most commonly mentioned purposes of processing:

	No. of Apps	**Name of Apps.**
To provide core services / enable app functions [49]	34	Clue, Flo, Frendo, Glow, Healofy, Menolife, Natural Cycles, Oky, SpotOn, Stardust, Period Calendar Period Tracker, Ovy Partner, Ovy BBT, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Me v PMDD, Pregnancy App & Baby Tracker, Pregnancy Tracker: Amma, Pregnancy + Tracker App, Moody Month: Cycle Tracker, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, kegg, Lioness, Lovense Remote, Medela Family - Breast Feeding, Oura, Tempdrop, We-Vibe, WHOOP
To provide customer service / respond to customer questions / communicating with the user	33	Clover, Clue, Flo, Frendo, FEMM Health and Period Tracker, Know Your Lemons, Menolife, Pregnancy App & Baby Tracker, SpotOn, Stardust, Period Calendar Period Tracker, Period Calendar - Period Tracker, Oky, Ovy Partner, Ovy BBT, Me v PMDD, Pregnancy Tracker: Amma, Ovulation & Period Tracker, Moody Month: Cycle Tracker, My Calendar – Period Tracker, Pregnancy + Tracker App, Elvie Trainer, Pump with Elvie, Garmin Connect™, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Lovense Remote, Lioness, kegg, Oura, Tempdrop, We-Vibe, WHOOP
To customise / personalise services	22	Clover, Flo, FEMM Health and Period Tracker, Health & Her, SpotOn, Kindara, Stardust, Period Calendar Period Tracker, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Pregnancy Tracker: Amma, Ovulation & Period Tracker, My Calendar – Period Tracker, Medela Family - Breast Feeding, Moody Month: Cycle Tracker, Elvie Trainer, Pump with Elvie, Garmin Connect™, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, kegg, WHOOP
To monitor and analyse trends / for statistical monitoring **For website and app**	30	Clover, Clue, Flo, Frendo, FEMM Health and Period Tracker, Healofy, Health & Her, Kindara, Know Your Lemons, Lovense Remote, Menolife, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Pregnancy App & Baby Tracker, SpotOn, Stardust, Medela Family - Breast Feeding, Moody Month: Cycle Tracker, My Calendar – Period Tracker, Oky, Elvie Trainer, Pump with Elvie, Garmin Connect™, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, kegg, Lioness, We-Vibe, Tempdrop, WHOOP

[49] The exact nature of these core services changes depending on the app, but they may include: processing health data to enable the tracking / prediction functions and processing account data to enable the user to sign in to the app.

analytics / statistical purposes		
For scientific / academic purposes	11	Clover, Clue, Kindara, Natural Cycles, Pregnancy App & Baby Tracker, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Me v PMDD, Moody Month: Cycle Tracker, kegg, WHOOP
To improve the app / service research & development	31	Clover, Clue, Glow, Health & Her, Kindara, Oky, Pregnancy App & Baby Tracker, taSpotOn, Stardust, Ovy Partner, Ovy BBT, Me v PMDD; Pregnancy Tracker: Amma, Lovense Remote, Ovulation & Period Tracker, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Moody Month: Cycle Tracker, My Calendar – Period Tracker, Pregnancy + Tracker App, Elvie Trainer, Pump with Elvie, Garmin Connect™, Embr Wave 2: Hot Flash Relief, kegg, Lioness, Oura, OvuSense, Tempdrop, We-Vibe, WHOOP.
Fixing problems & troubleshooting	14	Health & Her, Period Calendar Period Tracker, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovulation & Period Tracker, My Calendar – Period Tracker, Moody Month: Cycle Tracker, Pregnancy + Tracker App, Elvie Trainer, Pump with Elvie, Garmin Connect™, kegg, Lioness, We-Vibe
For marketing, advertising and promotional purposes	28	Clue, Flo, Frendo, Glow, Health & Her, Healofy, Kindara, Lovense Remote, Menolife, Natural Cycles, Pregnancy App & Baby Tracker, SpotOn, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Medela Family - Breast Feeding, Moody Month: Cycle Tracker, My Calendar – Period Tracker, Pregnancy + Tracker App, Elvie Trainer, Pump with Elvie, Garmin Connect™, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, kegg, Lioness, Oura, OvuSense, WHOOP
For newsletter services	7	Clue, FEMM Health and Period Tracker, Know Your Lemons, Ovy Partner, Ovy BBT, kegg, We-Vibe
For surveys, feedback and reviews	11	Clue, Health & Her, Know Your Lemons, My Calendar – Period Tracker, Pregnancy App & Baby Tracker, Pregnancy + Tracker App, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Elvie Trainer, Pump with Elvie, kegg,
To process transactions / billing / account management	15	Clover, Flo, Health & Her, Kindara, Menolife, Natural Cycles, Stardust, Moody Month: Cycle Tracker, Elvie Trainer, Pump with Elvie, Garmin Connect™, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, kegg, WHOOP,
To verify identity / register new users	11	Clover, Frendo, Health & Her Menopause, Moody Month: Cycle Tracker, Pregnancy + Tracker App, Elvie Trainer, Pump with Elvie, Garmin Connect™, kegg, Tempdrop, WHOOP
To comply with law / legal obligations	14	Frendo, Glow, Natural Cycles, Pregnancy App & Baby Tracker, SpotOn, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Menolife, Moody Month: Cycle Tracker, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, kegg, Oura, WHOOP
To comply with contractual obligations	8	Frendo, Period Calendar Period Tracker, Ovulation & Period Tracker, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, WHOOP.

Security / Detecting Fraud	10	Pregnancy App & Baby Tracker, Menolife, Natural Cycles, Elvie Trainer, Pump with Elvie, Garmin Connect™, Kegg, Lioness, Tempdrop, WHOOP,
To enable third party integrations and service (e.g., where people opt in to sync their app to another health / menstrual tracking app)[50]	5	Clover, Clue, Menolife, Garmin Connect™, Oura
To facilitate use of the Garmin Assistance Plus Service[51]	1	Garmin Connect™

Processing for wider research purposes (excluding internal product development)

One of the ways in which certain femtech apps market themselves is through their ability to contribute towards better understanding of women's health, which has thus far been under-researched. This was reflected in some of the privacy policies, for example:

- **Natural Cycles:** *"Women's health is important to Natural Cycles and we invest in scientific research in sexual and reproductive health in order to advance women's health.*" [52]

[50] E.g. **Clue** "*If you have given your approval, Clue may interact with the Health app on your iOS device and read and/or write information between the Clue app and the Health app…You can choose if and to what extent your personal data is exchanged between Clue and the Health app by granting or revoking the relevant permissions in your Health app settings*"; **Oura** "*We process personal data you provide to Ōura to enable third party integrations, services, features, and offerings. For example, with your permission, our Products may integrate with third party services like Google Health Connect and Apple HealthKit, or our research partn*ers".

[51] This is a particular Garmin safety feature, which allows a smartwatch to automatically send the user's name and location to Garmin Response to an emergency response coordination unit that can contact local emergency services.

[52] Natural Cycles mentioned that they also conduct research to evaluate "the effectiveness and suitability of the App for different user groups". The results of the research are used to "communicate the benefits and limitations of Natural Cycles to healthcare professionals." Natural Cycles also "contributes to research carried out by selected universities, institutions and other parties by sharing anonymized and minimized data with them." Finally, it is mentioned that they "may analyze sensitive data in order to publicly share insights learned from aggregated data with the purpose of increasing the public knowledge and understanding of women's health and/or the menstrual cycle. This kind of publication is always based on aggregated anonymized data and as such doesn't contain any personal information." Kegg also had a similar provision mentioning that they invest in scientific research in sexual and reproductive health in order to advance women's health.

18 of the apps included in this study explicitly mentioned that data may be processed for (scientific) research purposes. Of these, four specified that any such processing would require the separate, specific consent of the user – additional to the consent indicating acceptance of the general privacy policy / use of the app. Flo indicated that separate consent would *sometimes* be obtained, "*for certain targeted academic or user research studies*" and the two Ovia policies noted that specific informed consent will be obtained where "*required by law*".

The majority of the policies (16 of the 18) specified that the data used for this purpose will be either "anonymised", "de-identified", "pseudo-anonymised" and / or "aggregated". There are significant differences among these techniques of anonymisation and their consequences and it should be clearly explained to users why a specific method was selected and why was it needed (for example, why is pseudo-anonymisation to be used instead of de-identification?). This might be particularly important for data subjects to decide if they wish to give their consent.

Of note is the following statement in the privacy policies for the two Ovia apps: "*Ovia may receive compensation for sharing de-identified or aggregate data*."

Overall, while investment in women's sexual and reproductive health is crucial and urgently needed, it is concerning that only a minority of Policies include a requirement for separate consent where the data provided by users is used for scientific research. In such instances, informed consent would require that users are provided with clear information as to what research is being undertaken using their data, who is involved in this, including potential funders of such research (Universities, private institutions/ governments, etc.), whether this is subject to ethics oversight and how they could withdraw their consent. Even more concerning is that fact that apps might receive compensation for sharing users data (even in a unidentifiable form). This reveals a troubling approach of femtech actors, essentially denying any agency or 'empowerment' to femtech users.[53] Finally, information about why a particular de-identification method was selected for data processed for research purposes and the differences between the alternative methods matters to users and the vagueness of the relevant information in Privacy Policies is problematic and undermines users' informed consent.

Joining the Dots: Specific Types of Data, Purposes for Processing and Legal Basis

There was substantial variance in approach taken to drawing connections between the specific types of data being processed, the specific processing purpose / activity and the legal basis for the processing.

Several policies drew no direct links, or linked only some of the information, as detailed in the table below.[54] This can be confusing for users to navigate.

[53] For a similar argument see, Katharine Kemp, 'Your Body, Our Data: Unfair and Unsafe Privacy Practices of Popular Fertility Apps, 2023, https://allenshub.unsw.edu.au/sites/default/files/2023-03/KKemp%20Your%20Body%20Our%20Data%2022.03.23.pdf, 19.

[54] Where all boxes remain blank, no links are made by that specific policy.

App Name	Links SPECIFIC TYPES OF DATA and LEGAL BASIS for processing	Links SPECIFIC TYPES OF DATA and PURPOSE for processing	Links PURPOSE and LEGAL BASIS for processing	Links ALL THREE together
Clover - Safe Period Tracker				
Clue period tracker & calendar	X	X	X	X
FEMM Health and Period Tracker		X		
Flo Period & Ovulation Tracker			X	
Frendo Endometriosis Tracker	Partially			
Glow Cycle & Fertility Tracker		X	X	
Healofy Pregnancy & Parenting		Partially		
Health & Her Menopause App	X	X	X	X
Kindara Fertility & Ovulation		X		
Know Your Lemons - Self Exam		X		
Me v PMDD		X		
MenoLife - Menopause Tracker				
Moody Month: Cycle Tracker				
My Calendar - Period Tracker		X		
Natural Cycles - Birth Control	X	X	X	X
Oky Period Tracker App		X		
Ovia: Fertility, Cycle, Health		X		

Ovia: Pregnancy & Baby Tracker		**X**		
Ovulation & Period Tracker				
Ovy Partner - Share your Cycle				
PCOS Tracker				
Period Calendar Period Tracker				
Pregnancy + | Tracker App		**X**		
Pregnancy App & Baby Tracker		**Partially**		
Pregnancy Tracker: amma		**Partially**		
SpotOn		**X**		
Stardust		**X**		
Elvie Trainer	**X**	**X**	**X**	**X**
Pump with Elvie	**X**	**X**	**X**	**X**
Embr Wave 2: Hot Flash Relief	**X**	**X**	**X**	**X**
Femometer - Fertility Tracker			**X**	
Garmin Connect™	**X**	**X**	**X**	**X**
Kegg		**X**		
Lioness Health		**X**		
Lovense Remote		**X**		
Medela Family - Breast Feeding	**Partially**			
Oura	**X**	**X**		
OvuSense				
Ovy				
Tempdrop	**X**	**X**		**X**
We-Vibe	**X**	**X**	**X**	**X**
WHOOP			**X**	

While the Period Calendar Period Tracker policy did not link the types of data to the relevant legal basis for processing, it did specify that this information could be provided upon request: *"In any case, We will gladly help to clarify the specific legal basis that applies to the*

processing, and in particular whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract."

8. Changes to the Privacy Policy

23 apps stated explicitly that they would notify users if 'material' / 'significant' changes are made to terms of the privacy policy. In addition, Glow Cycle & Fertility Tracker indicated that users will be notified if this is required by law. A further three apps mentioned that users **may** be notified of potential changes to their Privacy Policy (MenoLife - Menopause Tracker, Lioness Health & Lovense Remote). Notification may be through the app, or via email.

The apps dealt with changes to their privacy terms in a range of different ways. We have identified three main approaches in this regard:

- Apps that notify the user of change and ask for consent

Examples:

- MenoLife - Menopause Tracker: "*The Owner reserves the right to make changes to this privacy policy at any time by notifying its Users on this page and possibly within this Application and/or - as far as technically and legally feasible - sending a notice to Users via any contact information available to the Owner…Should the changes affect processing activities performed on the basis of the User's consent, the Owner shall collect new consent from the User, where required*."

- Oky Period Tracker: "*We review our security measures and our Privacy Policy and we may modify our policies as we deem appropriate. If we make changes to our privacy practices, we will post a notification to the Oky website and app alerting you that the Privacy Policy has been amended. Such changes will be effective immediately upon posting them to the Oky app and website. For this reason, we encourage you to check our Privacy Policy frequently.*"

- Apps that notify the user only when the change is considered material, placing the onus on the user to stop using the service if they do not consent to the changes.

Example:

- **Oura:** *"We reserve the right to update this Policy from time to time at our sole discretion, but if we do, we'll let you know about any material changes either by notifying you on our Site or by sending you an email or push notification. If you keep using Ōura services after a change, your continued use means that you accept any such changes."*

- Apps who place the onus on users to check the website for changes, and then to stop using the service to if they do not consent to these.

Examples:

- **Embr Wave 2: Hot Flash Relief:** *"Our Services may change from time to time. As a result, we may need to change this Privacy Policy. We reserve the right to update or modify this Privacy Policy at any time and without prior notice. We will post any revised Privacy Policy on our website with an "effective date" indicating when the changes will take effect. We encourage you to review this Privacy Policy periodically."*

The third type of practice, and possibly the second one as well, is a cause for concern; it banks on users' passivity and thus undermines the user's free and genuine continuous consent to the uses of the data from the moment that the changes are in effect (at least where the changes are material).

9. Processing of Children's/ Girls' Personal Data

Femtech apps are often used by minors/ girls to monitor menstruation, sexual and reproductive health. We analysed the privacy policies to see if they mentioned the processing of children's data and, if so, how. Regarding the processing of children's data, the GDPR states that the processing of a child's data is only permissible if the child is over 16.[55] For UK GDPR, the child must be over 13.[56] In both cases, the data of children below the specified age is permissible only with consent of the child's parent / legal guardian.

Children's data processing (apps)

Processing of children's data not mentioned	**Minimum age 10**	**Minimum Age 13**	**Minimum Age 16**	**Minimum Age 18**	**Relative to Jurisdiction**	**Mention Parental involvement /Consent**
6 Healofy; Health and Her; Know Your Lemons; MenoLife; My	1 Oky[57]	6 FEMM; Ovulation Period Tracker; PCOS; Period Calendar Period Tracker;	2 Glow; Me v PMDD	2 Frendo; Natural Cycles[58]	10 Clover; Clue; Flo; Kindara; Moody Month; Ovia: Fertility, Cycle, Health; Ovia Pregnancy and Baby	Clover; Clue; FEMM; Frendo; Glow; Me v PMDD; Oky; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy

[55] GDPR Art 8.
[56] UK GDPR. Art 8.
[57] Note that Oky doesn't collect user data so regulation regarding processing child data won't apply. This also is not mentioned in the privacy policy, but is mentioned in the terms and conditions.
[58] Natural Cycles doesn't mention this in the privacy policy, but does discuss child data in the terms of service.

Calendar; Ovy		Spot On; Stardust			Tracker; Pregnancy + | Tracker App; Pregnancy App and Baby Tracker; Pregnancy Tracker: amma;	and Baby Tracker

Children's data processing (wearables)

Processing of children's data not mentioned	**Minimum Age 16**	**Minimum Age 18**	**Minimum Age 21**	**Relative to Jurisdiction**	**Mention Parental involvement/ Consent**
4 Medela; Oura Ring; Ovusense; We-Vibe	1 Tempdrop	4 Elvie Pelvic Floor; Elvie Smart Breast Pump; Lioness; Lovense;	1 Kegg	5 Embr Wristband; Femometer; Garmin Lily; Whoop	Embr Wristband; Lovense;

32 apps and wearables in total (21 apps, 11 wearables) mentioned processing children's data in their privacy policies, while 10 apps / wearables (6 apps, 4 wearables) did not make any mention of this. Two apps (Natural Cycles - Birth Control, and Oky Period Tracker App) did not mention processing children's data in their privacy policies, but did mention it in their Terms and Conditions.

Of the apps that mentioned processing children's data, some stated a minimum age a child needed to be in order to use the app / wearable. However, h*ow* age verification is to be ascertained was not usually explained.[59]

The majority of surveyed apps stated multiple different ages for different jurisdictions. For example, Flo set a general minimum age of 13 for all users: "*The Services are not intended for children, and we do not knowingly collect personal information from children under 13 years old through the Services*." But it also set a specific age for those in the EAA and UK: "*Due to legal requirements, we do not allow the use of the Services by residents of EEA or the UK younger than 16 years old*."

[59] Moody Month Privacy Policy stated that "Where specific countries have set the consent age for disclosing personal data to between 14 and 16 years of age under European Commission guidance, our app is formatted to disallow sign-up to use the MOODY App from those countries, in line with the prescribed age, based on a user location.". Available at: https://moodymonth.com/privacy-statement

Clover made similar claims: "*Age limitation for EU residents. Due to requirements of the GDPR, you shall be at least 16 years old in order to use the App. To the extent prohibited by applicable law, we do not allow use of the App by the EU residents younger than 16 years old.*"

Parental consent was mentioned in the policies of ten apps and two wearables. For instance, Me v PMDD stated that it "*does not knowingly collect or use personal data from children under the age of 16, without parental consent*." Likewise, Frendo noted: "*If you are under 18, you may use our website only with consent from a parent or guardian*." Oky - which had the lowest age restriction - stated that the app could be used by those above 10, but that those under 16 should get parental consent: "*Oky is targeted at young people from ages 10 and older. If you are under 16 years old, we encourage you to discuss your use and engagement on the Oky app with your parents or guardians and make sure that they consent to your use of the Oky app*."

In other cases, the privacy policies specified that girls could use a period tracking provided that a parent inputted the data and/or managed the account on their behalf. This was stated by FEMM:

"We do not collect Personally Identifiable Information from any person we actually know is under the age of 13. A parent or guardian, however, may use FEMM to establish a fertility record for a minor."

After stating that a parent could set up a fertility record on behalf of their child, FEMM state that:

"*The parent or guardian is solely responsible for providing supervision of the minor's use of FEMM. The parent or guardian assumes full responsibility for ensuring that the registration information is kept secure and that the information submitted is accurate. The parent or guardian also assumes full responsibility for the interpretation and use of any information or suggestions provided through FEMM for the minor. EU citizens aged 13-15 must have a parent or guardian consent to the use of data as outlined in this policy and needed for use in the App*."

This could be problematic in cases where teenage girls' choices and bodies are under the surveillance of their families, including parents and guardians.

Two wearables (Embr Wristband and Lovense) also mentioned parental involvement, with Embr stating: "*We recommend that persons over 16 but under 18 years of age ask their parents for permission before using the Services or sending any information about themselves to anyone over the Internet*." Lovense stated that: "*We encourage parents and legal guardians to monitor their children's internet usage and to help enforce our Privacy Policy by instructing their children under the age of 18 never to provide Personal Data to the Services*."

Several policies stated that they did not process the data of children under the minimum user age 'knowingly', and that, if they became aware that they are processing data of someone under the minimum age, they would stop this immediately. Other policies instructed that a child could engage with the app if the parent took responsibility for managing the child's account, and

inputting all their data. It appears that policies that allowed the processing of children's/ girls' data with parental involvement, were more concerned with how the child used the app, rather than with the gendered risks this processing might entail (if parental consent is sufficient for the processing of a child's data, there is no problem in principle with processing such data as far as these companies are concerned).

Beyond this, none of the apps / wearables that mentioned children's data offered any information about additional protections they had in place for processing children's data.

Use of femtech apps by teenagers also raises questions around girls' sexual and reproductive literacy and education and ultimately empowerment and autonomy which for some girls might need to be pursued beyond the will of their parents/ guardians. Some Terms of Service mentioned that the app is "not for use by minors" or "does not promote sexual activity among minors". Flo stated that they carefully monitor the information they make available to users between the ages of 13 and 17. Pregnancy Tracker: amma also stated that it did not promote sexual activity amongst minors and that the information was not directed at a particular audience and was intended for information purposes only. Interestingly, Health and Her was the only app that mentioned children data in the Terms of Service but not in the Privacy Policy.

10. Data Storage

37 of the 42 policies analysed made a reference to the duration of data retention.[60]

Where data retention / storage was mentioned, a range of different approaches was taken to determining and articulating the length of the data-storage period. Some of the policies provided lengthy explanations as to how storage length was determined:

- **Glow:** "*We generally retain personal information to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for fraud prevention purposes. To determine the appropriate retention period for personal information, we may consider factors such as the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements. When we no longer require the personal information we have collected about you, we may either delete it, anonymize it, or isolate it from further processing.*"

- **Oura:** "*The retention period for your personal data generally depends on the duration of your Ōura account lifecycle. Your personal data will be deleted when it is*

[60] The policies which do not mention this specifically are: Kindara Fertility & Ovulation, Know Your Lemons - Self Exam, Me v PMDD, My Calendar - Period Tracker and OvuSense.

no longer needed for the purpose for which it was originally collected, unless we have a legal obligation to retain data for a longer period of time. For example, your measurement data regarding your sleep, readiness, and activity is stored only so long as your Ōura account is active. Ōura also has legal obligations to retain certain personal data for a specific period of time, such as for tax purposes. These required retention periods may include, for example, accounting and tax requirements, legal claims, or for any other legal purposes. Please note that obligatory retention periods for personal data vary based on the relevant law."

However, despite the level of detail provided above, these policies fail to provide a clear retention time period to users.

Furthermore, some Policies stated broadly that information would be kept for as long as is required to fulfil the purpose for which it was collected. Such wording also fails to provide any clarity and certainty to users.

As mentioned above, Euki did not link sexual and reproductive data with other identifiable information (e.g., email address) and the app further stated "*To protect your privacy, Euki gives you the option of deleting the data you log in the calendar. This will help make sure your sensitive information will not be used against you*". The Euki app further provided the options to users to 'Set frequent data deletion' or to 'Delete all data now'.

Besides specifying a clear retention period, it is also important to understand what Policies mention as to what happens to the data once the retention time period has passed. Some apps, such as Clue specified that data would be deleted "*as soon as it is no longer required for the purpose for which it was collected".*

FEMM stated: **"***FEMM will retain personal information shared for at least six years as described in this Policy unless you request deletion of your information.*"

Flo mentioned: "*If you choose to delete the App from your device or your account becomes inactive, we will retain your personal data for a period of three years in case you decide to reactivate the Services or reinstall the App. After three years of inactivity and not using the App, we will delete your personal information. While this is the Flo data retention standard, you can still ask for your data to be deleted at an earlier date by contacting us. The App covers different periods of users' lifecycle; therefore, retention of your data is needed in some cases to secure your smooth experience with other App functions (e.g., switching to pregnancy mode after cycle tracking).*"

The Clover policy only made brief and non-specific mention of the storage / retention of data, stating that *"When you deactivate your User Account, some or all of the information stored and maintained as part of your account may be retained on our servers, including the User Content uploaded via the Services".* The use of terms such as 'some or all of the information' and 'may' is confusing and misleading. More importantly, privacy policies contravene the GDPR if they do not provide clear retention periods or provide for unnecessarily excessive

retention periods, if they fail to give an indication of whether the data is deleted once the retention period has expired and where they do not provide for any retention periods but continue to maintain the data even after the user has deactivated her account.

11. Data location

30 of the apps did not specify the location where the data is stored. MenoLife - Menopause Tracker explicitly noted that information about storage location is complicated: *"Some of these [third party]services work through geographically distributed servers, making it difficult to determine the actual location where the Personal Data are stored."*

Data location might, however, provide important information to users, among others, regarding the applicability of relevant laws and the issue of potential data transfers to third countries (where relevant). For example, Euki mentioned that it "*does not store any of your data on a cloud. It lives on your phone and in the app and is not shared anywhere else*".

The table below details the information provided by those policies which provided specific data storage location information. The specificity varies, and some policies only mentioned specific locations for certain types of data:

App Name	Location of Data Storage
Clover - Safe Period Tracker	Finland and Germany
Clue period tracker & calendar	European Union
FEMM Health and Period Tracker	USA
Kindara Fertility & Ovulation	USA
Know Your Lemons - Self Exam	**Cookie data**: stored in the United States on Google servers. **Other data**: not specified.
Me v PMDD	**Analytics data:** USA **Personal and health data:** not specified, "on our servers"
Moody Month: Cycle Tracker	"inside and outside the European Economic Area ("EEA"), including the United States of America"
Ovia: Fertility, Cycle, Health	USA
Ovia: Pregnancy & Baby Tracker	USA
Pregnancy Tracker: amma	"including but not limited by the following jurisdictions: SAR Hong Kong, the Russian Federation, the United Kingdom of Great Britain and

	Ireland [sic], United States of America, European countries, countries of Latin America"
Garmin Connect™	USA, UK and/or Australia.
Medela Family - Breast Feeding	Ireland and the Netherlands. Additionally, US and Canadian user data will be stored in the USA,
Tempdrop	"throughout the globe"

12. Data Sharing

Information about femtech data sharing often seemed to be complex to discern. For example, as the table below demonstrates several apps used ambiguous language regarding their data sharing practices. This can contribute to lack of clarity, and risks undermining informed consent – as the question of whether or not data will be shared is a material one.

	Number of apps	**List of apps**
Use "may" share data	**20**	Clover - Safe Period Tracker; Frendo Endometriosis Tracker; Glow Cycle & Fertility Tracker; Healofy Pregnancy & Parenting; Health & Her Menopause App; Kindara Fertility & Ovulation; Know Your Lemons - Self Exam; Natural Cycles - Birth Control; Pregnancy + | Tracker App; Pregnancy App & Baby Tracker; Pregnancy Tracker: amma; SpotOn; Stardust; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Lovense Remote; Medela Family - Breast Feeding; WHOOP
Use "may" share in specific instances[61]	**7**	FEMM; Flo; My Calendar - Period Tracker; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy & Baby Tracker; Moody Month: Cycle Tracker; Lioness
Do not use "may" share	**15**	Clue period tracker & calendar; Me v PMDD; MenoLife - Menopause Tracker; Oky Period Tracker App; Ovulation & Period Tracker; Ovy Partner - Share your Cycle; PCOS Tracker; Period Calendar Period Tracker; Garmin Connect™; Kegg; Oura; OvuSense; Ovy; Tempdrop; We-Vibe,

As seen above, the majority of policies mentioned that they 'may' share data with third parties. Fewer apps avoided such ambiguous language by either decisively mentioning that the do share data (rather than leaving it ambiguous through the use of open language (e.g. Oura: *"we share your data with…"* or by stating that the app does not share data with third parties (e.g. Period Calendar Period Tracker: *"We NEVER share the information you are tracking in our app (e.g. your health information) with any third party"*).

[61] For example, the Ovia: Fertility, Cycle, Health and Ovia: Pregnancy & Baby Tracker Policies state: "*We may share data with our parent company Labcorp and with companies under common control, and with any successors in the event of merger, acquisition, asset sale, or similar transaction*" and "*We may share device data with social media networks to measure the effectiveness of advertising on those networks*" but in other places in use more precise language ("*we share*").

Only eight apps comprehensively listed all of the third parties who gained access to the data.[62]

The policies which did not provide a comprehensive list of all third parties with whom data is shared provided different levels of detail: some merely listed the general categories of third parties; some listed the key third parties by offering examples of some third parties but stopping short of providing a comprehensive list; some merely offered a few examples and some provided no detail (e.g. the PCOS Tracker simply stated that data is shared with "*trusted service provider*s"). Healofy Pregnancy & Parenting policy directed users to contact the data controller to request a full list of third parties with access to the data.

Sharing Data with Law Enforcement

A significant privacy related concern is that femtech data might be shared with law enforcement authorities, and used to support abortion prosecution or to undermine reproductive health autonomy. This has become a major concern in the USA following the Supreme Court decision in *Dobbs v Jackson,*[63] which overturned *Roe v Wade*[64] and paved the way for the criminalisation of abortion in a number of states. It is notable that abortion remains an offence in England and Wales - and there is evidence that police have, in some cases, requested access to period tracker data during abortion investigations.[65] Abortion laws vary across Europe,[66] but it is important to note that there remain restrictions on lawful termination in a number of countries - most notably Poland, where a decision by the Constitutional Tribunal in 2021 severely restricted the situations in which abortion could be lawfully accessed.[67]

The table below indicates that the vast majority of apps were explicit in the fact that they share data with law enforcement if required by law. Stardust was an outlier in this regard, stating explicitly: "*What happens if law enforcement sends us a subpoena for your data: We cannot prevent the government from issuing a subpoena. However, in such a case we would not be able to produce your period data because we cannot connect it to your login information*."

Willing to respond to law enforcement request if required by law	33	Clover - Safe Period Tracker, FEMM Health and Period Tracker, Flo Period & Ovulation Tracker, Frendo Endometriosis Tracker, Glow Cycle & Fertility Tracker, Healofy Pregnancy & Parenting, Health & Her Menopause App Kindara Fertility & Ovulation, Know Your Lemons - Self Exam, MenoLife - Menopause Tracker, Moody Month: Cycle Tracker, My Calendar -

[62] Kindara Fertility & Ovulation, Me v PMDD, MenoLife - Menopause Tracker, My Calendar - Period Tracker, Ovy Partner - Share your Cycle, Stardust, Ovy BBT, Tempdrop (users were directed to a different document for this).

[63] Dobbs v Jackson Women's Health Organization 597 US 215 (2022).

[64] Roe v. Wade, 410 U.S. 113 (1973).

[65] Phoebe Davis, 'British police testing women for abortion drugs' (*Tortoise Media,* 30 October 2023) <https://www.tortoisemedia.com/2023/10/30/british-police-testing-women-for-abortion-drugs/> accessed:

[66] https://reproductiverights.org/wp-content/uploads/2020/12/European-abortion-law-a-comparative-review.pdf

[67] Amnesty International, 'Poland: Vote is a significant step towards providing access to safe and legal abortion' (12 October 2024) <https://www.amnesty.org/en/latest/news/2024/04/poland-vote-is-a-significant-step-towards-providing-access-to-safe-and-legal-abortion/> accessed 9th September 2024 - note, there is optimism following the 2024 Polish elections that the restrictions may soon be eased to some extent.

		Period Tracker, Natural Cycles - Birth Control, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovulation & Period Tracker, PCOS Tracker Period Calendar Period Tracker, Pregnancy + Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, SpotOn, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Garmin Connect™, Kegg, Lioness Health, Lovense Remote, Medela Family - Breast Feeding, Oura, Tempdrop, WHOOP
No data to provide to law enforcement	1	Stardust
Not mentioned	8	Clue, Me v PMDD, Oky*, Kegg*, OvuSense, Ovy Partner, Ovy BBT, We-Vibe

** While Oky and Kegg do not specifically mention whether they will share data with law enforcement, they do note in more general terms that information may be used to respond to legal requests / fulfil legal obligations.*

While ultimately complying with law enforcement requests where there is a legal obligation to do so, some of the apps demonstrated a greater appreciation of the potential implication of sharing intimate data in this way. A number of apps indicated that they would carefully review requests to ensure there is a legitimate basis and specific investigative purpose justifying the request: Period Tracker Period Calendar, Ovulation and Period Tracker, Natural Cycle, WHOOP. Clover required receipt of "appropriate documentation" before they would comply with requests.

A small number also indicated that they would notify users before sharing any data with authorities where they get a request to do so: FEMM (unless notification is prohibited), Natural Cycles (unless notification is prohibited), Lioness (unless notification is prohibited) and Oura (where request is received). Of course, the actual significance of this depends on the extent to which relevant authorities routinely prohibit notification when requesting access to data. Most significantly, Natural Cycles, Pregnancy App & Baby Tracker, Oura[68] and WHOOP[69] indicated that they would resist such requests. For example,

[68] *"We …reserve the right to disclose personal information under certain specific circumstances, including: ...To comply with valid legal requirements. Oura will oppose any request to provide legal authorities with access to user data for surveillance or prosecution purposes, and will notify users if we receive any such request."*

[69] "*Like all other companies, WHOOP may from time to time receive requests for member data from third parties, like governmental entities (including law enforcement) and private parties engaged in civil litigation. Here are the key principles we stand by when evaluating these requests:*

- *WHOOP will never voluntarily disclose member data in response to a request by a governmental entity or civil litigant.*
- *WHOOP will never provide any governmental entity or civil litigant with direct access to our members data.*
- *WHOOP will never provide copies of member data held by WHOOP to any governmental entity or civil litigant without a valid, narrowly tailored, and legally-binding request (e.g., subpoena, warrant or court order).*
- *If WHOOP receives a request for a members (sic) data, we will provide notice to the member by sending an email to the email address we have on file for that member.*
- *WHOOP is prepared to fight to protect our members (sic) privacy in court if necessary. We will reject, challenge or object to any data access request from a governmental entity or civil litigant that we believe is invalid, overly broad, unclear or otherwise inappropriate."*

- **Natural Cycles:** "*Natural Cycles will provide personally identifying data in response to a third-party inquiry only if required by a valid legal process, but will take all possible steps to keep your data private. Natural Cycles will contest the disclosure of your personal data in response to a third-party inquiry to the extent that a reasonable ground for objection exists. Natural Cycles will provide you with prompt prior notice of such a request, to the extent legally permitted, so that an order for relief may be requested. If Natural Cycles reasonably determines that such disclosure is still legally required, then it will seek a confidentiality designation protecting the disclosure, and will only disclose the portion necessary and at the required time.*"

- **Pregnancy App & Baby Tracker***:* "*We may disclose your User Information*[70] *to legal and regulatory authorities (including law enforcement agencies and courts) to respond to legal requests or orders, comply with applicable law, or exercise or defend our legal rights. We are mindful of your legal rights and may act to protect them. We may object to legal requests or orders that are overbroad, infringe your or our protected rights, or otherwise exceed legal authority."*

Interestingly, the Euki app stated that "*If someone asks you to open Euki and you don't want them to see your data, enter [a certain code] when you open the app and we'll display a fake screen.*"[71] This appears to be a further way to resist legal obligations, but also intimate partner or family surveillance of women's sexual and reproductive data.

13. Targeted Advertising

Sharing data for **personalised ads** is often considered essential to the business models of several digital technologies, including femtech. The Table below details data processing for targeted advertising.

Is data tracked or shared for targeted / personalised advertising?		
Yes	27	Clover - Safe Period Tracker, Clue period tracker & calendar, FEMM Health and Period Tracker, Frendo Endometriosis Tracker, Glow Cycle & Fertility Tracker, Healofy Pregnancy & Parenting, MenoLife - Menopause Tracker, My Calendar - Period Tracker, Natural Cycles - Birth Control, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovulation & Period Tracker, Ovy Partner - Share your Cycle, Period Calendar Period Tracker, Pregnancy + Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, SpotOn, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Garmin Connect™, Kegg, Lovense Remote, Medela Family - Breast Feeding, Ovy BBT, WHOOP

[70] *"User information is defined expansively in the privacy policy as including personal data and a range of other information (e.g. device ID, advertising ID, browsing history and approximate location), but notably excludes health or other special category data."*

[71] The code has been redacted.

Yes - but explicitly excludes certain data from this	3	Kindara Fertility and Ovulation (it stated that it excludes personal information, but this statement is unclear), Moody Month: Cycle Tracker (it states that excludes health data); Oura (it states that it excludes health data)
No	1	Flo
Not mentioned	11	Health & Her Menopause App, Know Your Lemons - Self Exam, Me v PMDD, Oky Period Tracker App, PCOS Tracker, Stardust, Femometer - Fertility Tracker, Lioness, Ovusense, Tempdrop, WeVibe.

The majority of policies recognised that data is shared for personalised ads. In a number of cases this was 'not mentioned'. It might be possible to infer that data is not used this way from the other details of the policy. However, even if data is in fact not shared for this purpose, this should be stated clearly in the privacy policy- users should not be required to draw inferences.

In some cases, such as Frendo and Healofy Pregnancy and Parenting, the data was tracked and used by third parties for advertising purposes; in others, this was done by the app provider themselves.

The Information Commissioner's Office has noted that, "over half of people (54%) who use the apps believed they had noticed an increase in baby or fertility-related adverts since signing up."[72] Moments of change in the reproductive life course, such as the menstruation, pregnancy and menopause, are "amongst the few life stages where people are open to "brand capture"[73] and thus the kinds of intimate data generated by femtech apps can be considered as "a valuable form of currency"[74] and as "advertising gold."[75] This can be perceived by users as an invasion of privacy, and can also have specific harmful consequences whereby those who have had an abortion or experienced pregnancy loss or stillbirth receive targeted ads for baby products.[76]

Opting out from targeted advertising

Of the 30 apps which explicitly acknowledged that they tracked or shared data for targeted advertising, or allowed a third party to do so, eleven clearly specified an option for users to opt-out of targeted advertising (or elements thereof).[77]

[72] Information Commissioners Office (ICO), 'PACE Project: Fertility & Menstruation Apps – Internal Report' (Redacted Version available at https://ico.org.uk/media/about-the-ico/disclosure-log/4030017/femtech-report_redacted.pdf) 28.

[73] Danielle Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (Chatto & Windus 2022) 18.

[74] Eliza Hammond & Mark Burdon, 'Intimate Harms & Menstrual Cycle Tracking Apps' (2024) 55 *Computer Law & Security Review* 1, 10.

[75] Danielle Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (Chatto & Windus 2022) 14.

[76] Lucy Purdon, 'Unfinished Business: Incorporating a Gender Perspective into Digital Advertising Reform in the UK and EU' (Mozilla Foundation, 2023) 40. For further discussion on the relevant harms: Anastasia Siapka, Maria Tzanou and Anna Nelson, 'Re-imagining data protection: Femtech and gendered risks in the GDPR' in R. Costello and M Leiser (eds.) *Critical Reflections on the EU's Data Protection Regime: GDPR in the Machine*, (Hart, 2024), 101.

[77] Clue period tracker & calendar, FEMM Health and Period Tracker, Glow Cycle & Fertility Tracker, MenoLife - Menopause Tracker, Moody Month: Cycle Tracker, My Calendar - Period Tracker, Natural Cycles - Birth Control, Period Calendar Period Tracker, Pregnancy Tracker: amma, SpotOn, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Garmin Connect™, Kegg, WHOOP.

A small number of policies referenced self-regulatory instruments created by industry groups, for digital advertising (for example, My Calendar - Period Tracker,[78] WHOOP and Spot On).[79]

Four additional apps engaged with opt-out to some extent. These were not included in the primary total due to either the ambiguity or jurisdictionally limited scope of their opt-out offer. For example,

- **Clover** has been excluded from the table above because of the ambiguous language contained within their policy; if users wish to access information about their "*choices as to not having your information used*" by third party companies for these purposes, they are required to contact "*the respective company's administrator or webmaster.*" It is not clear whether users will be provided with the choice to opt out if they do make this contact. It is also left to the user to find the relevant contact details; these are not detailed in the policy.

- **Pregnancy App & Baby Tracker** has been excluded because it is unclear whether the opt-out option is available to those outside of California.

- **Ovia: Fertility, Cycle, Health** and **Ovia: Pregnancy & Baby Tracker**, have been excluded because they limit the right to opt-out the "*sale or sharing of your data for personalized advertising*" to US residents in States where the law requires this option: namely California, Colorado, Connecticut, Virginia and Utah.

It is important to note that, as a number of policies specified, opting out of targeted advertising, does not mean opting out of all advertising. For example, the WHOOP policy stated*: "Opting-out of interest-based advertising does not mean that you will no longer receive online ads. It only means that such ads will no longer be tailored to your specific viewing habits or interests. You may continue to see ads on and about the Service."*

Data processed for advertising by third-parties

The Table below sets out the policies which mentioned that they process data for the purposes of third-party advertising.

[78]The policy states: *"we are members of the Digital Advertising Alliance (DAA) (http://www.aboutads.info/), European Digital Advertising Alliance (http://www.edaa.eu/) and Japan Interactive Advertising Association (JIAA) (http://www.jiaa.org/). Therefore, we adhere to the cross-industry Self-Regulatory Principles for Online Behavioral Advertising, the IAB Europe EU Framework for Online Behavioral Advertising, and JIAA Behavioral Targeting Advertising Guidelines".*

[79] Whoop complies with "the Digital Advertising Alliance Self-Regulatory Principles for Online Behavioral Advertising"; SpotOn policy notes "to learn more about interest-based advertising and how you may be able to opt-out of some of this advertising, you may wish to visit the Digital Advertising Alliance's (DAA) resources and/or the Network Advertising Initiative's (NAI) online resources, at www.aboutads.info/choices or http://www.networkadvertising.org/choices/".

Data processed for advertising by third-parties	No. of Apps	Name of Apps
Yes	**21**	Clover - Safe Period Tracker, FEMM Health and Period Tracker, Frendo Endometriosis Tracker, Glow Cycle & Fertility Tracker, Healofy Pregnancy & Parenting, MenoLife - Menopause Tracker, My Calendar - Period Tracker, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovy Partner - Share your Cycle, Pregnancy + | Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, SpotOn, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Kegg, Lovense Remote, Ovy BBT
Yes, but excluding health / wellness data	**3**	Clue period tracker & calendar (health data), WHOOP (wellness data), Flo (health data)
Only with additional consent	**2**	Period Calendar Period Tracker, Ovulation & Period Tracker
No	**1**	Oura
Not mentioned	**15**	Health and Her**, Kindara Fertility & Ovulation**, Know Your Lemons - Self Exam*, Me v PMDD*, Moody Month: Cycle Tracker, Natural Cycles - Birth Control*, Oky Period Tracker App*, PCOS Tracker*, Stardust*, Garmin Connect™*, Lioness*, Medela Family - Breast Feeding*, OvuSense*, Tempdrop*, WeVibe*.

[*] These Policies stated clearly that data would only be processed by third parties in the ways outlined in the policy, unless separate and explicit consent was obtained (e.g."*Me v PMDD will not share your personal tracking data with third-party services beyond what is outlined below*"). On the basis of this, it might be possible to *infer* that data is not processed for advertising by third parties where this is not explicitly mentioned in the policy. This cross-referencing to different provisions of the Privacy Policy is confusing and overall fails to provide adequate certainty to users.

[**] These Policies include broad statements about the reasons why data may be shared with / processed by third parties. Such statements are problematic under the GDPR because they are vague and ambiguous and undermine transparency and certainty. For example, the Kindara Policy included a broad statement which could permit the following:

> *"Website, Web App, or App Usage. Kindara and its vendors Google, Mailchimp, Facebook and HubSpot may observe your activities, preferences, and transactional data (such as your IP address and browser type) as well as content you have viewed during your use of the Service. We may use this data for any purpose unless we tell you otherwise in connection with a particular Service. While we may collect or log this information, we do not identify you or match this non-Personal Information with your other Personal Information."*

This statement is concerning because it shows the invisible tracking that femtech users are subjected to. This raises doubts about the lawfulness and transparency of processing as well as the level of agency or choice that the user is provided given the obscure terminology ('may') and the fact that separate consent is not sought in this case.

We observe that although third-party sharing is often considered essential to the business models of several digital technologies, when performed in the femtech context, it predominantly relies on and affects women.[80] Such marketing practices for which this data sharing is employed are gendered, capitalising on data related to women's reproductive milestones and enabling the segmentation of marketing targets into reproduction-related profiles (e.g., 'heavy purchaser of pregnancy tests' or 'infertility/IVF').[81] Based on these data and profiles, marketers make assumptions about women's desires and likely purchases, with the prevalent assumptions being that they desire to conceive or that they will desire baby products nine months after conception. These assumptions feed into advertising practices which, unbeknownst to the femtech users on whose data they rely, might be experienced by women as unnecessary and creepy or even shameful and upsetting, depending on their individual circumstances.[82] For instance, being targeted with Facebook ads about unwanted baby products might be highly distressing for a woman who has just suffered a stillbirth. As we argued elsewhere,[83] this sharing of the data with third parties without explicit consent is an example of a gendered individual data risk / harm because it has an individual adverse effect relating to gender-through its inextricable connections to women's reproductive life.

Data shared with third-parties for profit

There are a number of different third parties who may be interested in purchasing femtech app user data, including advertisers, data brokers and information resellers.[84]

The privacy policies of the two Ovia Apps (Ovia: Fertility, Cycle, Health and Ovia: Pregnancy & Baby Tracker), for example, specified that they sell / share online identifiers and IP addresses with "*advertising networks*, *advertising platforms*, *advertising technology providers and advertisers*" for the purpose of "*sale or ad sharing.*"

In some cases it appears that third party partners directly profit from user's data - rather than the app company themselves. For example, the Kegg policy specified that while the company *"never sell[s] the personal information"* of their users, it may share information with third party partners who may generate profit from that data:

> "*It may be possible for our third-party business partners to combine cookies with other information in order to identify your email address or other personally identifiable information about you. For example, the cookies may reflect de-identified demographic or other data linked to data you voluntarily have submitted to us, e.g., your email address, which we may share with a data provider solely in hashed, non-human readable form. By using our Service, you*

[80] Siapka, Tzanou and Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.
[81] Ibid.
[82] Ibid. For the broader trade-off involved in personalised default rules (alleged increased efficiency, decreased privacy and the problem of profiling, stratification and tracking see Tsachi Keren-Paz, 'The Uncreditworthy's Tale: Personalized default rules and the problem of tracking' (2020) 42 *Tel Aviv ULR* 421.
[83] Siapka, Tzanou and Nelson, ibid.
[84] As listed, for example, in the Stardust Privacy policy at [2]: Stardust, 'Privacy Policy' <https://stardust.app/privacy-policy.html> accessed 17 August 2024.

> *agree that us and our third-party partners may store, sell, port, combine with other data, monetize, utilize and otherwise use either (i) the personally indefinable information about you that we share with them, or (ii) the personally identifiable information they discover and/or identify as described above.*"

The PCOS Tracker, stated that:

> *"In addition, the Application may collect certain information automatically, including, but not limited to, the type of mobile device you use, your mobile devices unique device ID, your mobile operating system, the type of mobile Internet browsers you use, and information about the way you use the Application."*

Five apps described 'combining' the data they gained about the user, including from other sources besides the app / wearable. For example, Pregnancy+ and Baby Tracker stated:

> "*We may combine your personal data, including account data, other data provided by you, Device data, cookies, location data, data collected during your interactions and usage of the Philips digital channels, such as social media, websites, emails, apps and connected products, IP address, cookies, device information, communications you click on or tap, location details and websites you visit."*

The use of cookies was also mentioned in this context. For example, after stating that "*We automatically track certain information about you based upon your behavior on App*", Healofy also stated that "*We will use cookies on our App similar to other lending websites / apps and online marketplace websites / apps. Use of this information helps Us identify You in order to make our App more user friendly*." 21 policies mentioned the use of cookies as a means of tracking users' activity. Some specified that the information tracked was 'non-personal', others specified that it was 'personal'. Most policies added that the user could disable cookies voluntarily, but doing so may affect the functionality of the app / wearable, and may lead to a user experience less tailored to them.

Some policies made it very clear that data is not shared with third parties. Some app presented this as a potentially important marketing point. For example, this was displayed prominently at the very top of Stardust's privacy policy:

WHOOP is interesting in this regard, because it explicitly recognised that data-selling is a business model which allows for free access to their services. They were explicit that their decision to run a service based on membership fees enables them not to sell personal data: "*Our business model is to provide highly valuable product experiences and services to our members in exchange for membership fees. As such, we never sell our members' personal data. This is our promise*" (WHOOP, Privacy Principles).

Also of note is how a number of policies defined selling of personal data. For example:

- **Ovulation and Period Tracker:** *"You have the right to opt out of sharing certain information with third parties who may only use your personal data for their purposes. Your right to opt-out applies only to information we "sell" to these third parties. In this context, "selling" does not mean exchanging information for money—we do not engage in such practices. "Selling" refers to the disclosure of information when a third party may use it for their own purposes, such as personalized advertising, including non-identifiable technical device information."*

- **My Calendar - Period Tracker:** "*As noted above, we do not sell or share any User Data. We may, however, provide Advertising IDs from your device to Advertisers. Under certain laws, including California law, the provision of Advertising IDs may constitute a sale of Person Information.*"

As Purdon observed some app developers give away the data for free (rather than selling it), knowing that in return "they can re-target existing consumers or analyse consumer behaviour for their own purposes."[85]

14. Femtech Business Models and Their Impact on User Experience

Femtech business models—free or paid/ premium services—often determine whether apps provide ads to users and/ or offer a different (normally more advanced) service/ functionality.

Eleven of 27 of the app-only femtech products offer a premium, paid service. There is not a premium version of the 'Period Tracker Period Calendar', but there is an option through the settings to pay £1 to "remove ads forever".

App Only

[85] Lucy Purdon, 'Unfinished Business: Incorporating a Gender Perspective into Digital Advertising Reform in the UK and EU' (Mozilla Foundation, 2023) 16.

App Name	Paid Version: Removes Ads?	Paid Version: Functionality Difference?
Clue period tracker & calendar	The app does not contain ads, even when free	Yes
Flo Period & Ovulation Tracker	Not mentioned in the list of premium benefits	Yes
Frendo Endometriosis Tracker	Not specified	Yes
Glow Cycle & Fertility Tracker	Yes "ad free"	Yes
Kindara Fertility & Ovulation	Not mentioned in the list of premium benefits	Yes
Moody Month: Cycle Tracker	Not specified	Yes
Ovulation & Period Tracker	Yes	Yes
My Calendar - Period Tracker	Not specified	Yes
Pregnancy + | Tracker App	Not specified	Yes
Pregnancy Tracker: amma	Yes ("turns off all ads")	Not specified
Stardust	Not specified	Yes

Paying for the premium version also stops the user from receiving in-app ads to subscribe / upgrade to this service. While this is an obvious point, it is also an important theme which could be clearly identified from our survey of users' reviews.[86] In particular, femtech users pointed out that in some apps the 'aggressive' promotion of the premium upgrades was unpleasant, and would significantly impede the functionality and their user experience of the app.[87]

Wearable-Associated Apps

When it comes to the apps associated with a wearable device, the business models are slightly different - owing to the fact that use of these apps requires the purchase of a physical device. There is no one-size-fits-all approach, however. In the case of Natural Cycles, the user can

[86] See our 'Femtech User's Reviews Research Report' (*forthcoming*).
[87] See for instance, "the push for buying premium is near harassment level", "amount it pushes upgrading feels like a bully tactic of "pay us to leave you alone."", "a near constant push to purchase a subscription", "incessant pop ups trying to sell you premium", "Unusable… unending urges to upgrade".

either pay for an annual app subscription and receive a free thermometer, or a month app subscription where they pay an additional initial 'one off payment' to purchase the thermometer. With the Oura Ring, the user purchases the device and the subscription (monthly or annual) separately. WHOOP takes a combined approach, where the user selects a membership option which includes an 'upfront cost' as well as a monthly one, and they receive a device as part of this. In the case of both the Elvie Breast Pump (app: Pump with Elvie) and Elvie Pelvic Floor Trainer (App: Elvie Trainer), the user only purchases the device; the apps are free to download and use.

Both Natural Cycles and WHOOP identify the need to pay for a subscription as a privacy enhancement practice:

- **Natural Cycles:** "*Unlike free apps, our monthly subscription helps protect you and your data*".[88]
- **WHOOP:** "*Our business model is to provide highly valuable product experiences and services to our members in exchange for membership fees. As such, we never sell our members' personal data. This is our promise.*"[89]

'Women-Owned' femtech (as a Marketing Tool)

A number of the companies emphasised the fact that they are 'women owned', such as:

- **Moody Month:** "*We are a women-owned and led company that values data privacy. Your data is not sold to third parties and is used only to provide you with the information you need to understand yourself better.*"[90]
- **Elvie:** "*Female-founded. Female-grounded.*"
- **Stardust:** "*Stardust is an astrological period tracker owned and operated by a team of four women based in New York City.*"

The following user reviews, which come from an app which is not women-founded/ owned, illustrate that this is something which does matter to some users: "…it's owned by men which is not illegal lol but personally it makes me feel uncomfortable that they founded a company to profit off of our periods", and "Recently found out this was made by a man, uninstalling and downloading an app made by women. Men already controlled and create everything the least they could do is keep their noses out of women's periods."[91]

The research found that, in general, apps and wearables founded/ owned by women are also in general careful about their compliance with relevant data privacy laws.

[88] Natural Cycles, 'Frequently Asked Questions' <https://www.naturalcycles.com/faqs> accessed: 26th September 2024
[89] WHOOP, 'Privacy Principles' <https://www.whoop.com/us/en/privacy-principles/> accessed 26th September 2024.
[90] Wendy Anderson, 'Meet Oky: The period tracker made for girls, by girls' (*The Case for Her*, 14 July 2020) <https://thecaseforher.com/blog/meet-oky-the-period-tracker-made-for-girls-by-girls/> accessed 25th September 2024.
[91] For further information on femtech users' reviews, see our relevant Report.

15. Data Subject Rights

A key aim of the GDPR is to empower individuals by giving them control over their personal data.[92] The data subject rights, included in Chapter III of the Regulation -right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, right to object) are seen as an important tool for achieving this aim.

Notably, while the majority of policies did make reference to some data subject rights, in many cases they did not comprehensively address all the rights. 24 of the policies mentioned (affirmatively) *all* the rights listed in the table below,[93] while seven of them mentioned *none* of these rights.[94]

	No. of Apps	**Name of Apps**
Privacy Policies Mentioning Art 15: *Right of access by the data subject*	**35**	Clover - Safe Period Tracker, Clue period tracker & calendar, FEMM Health and Period Tracker, Flo Period & Ovulation Tracker, Glow Cycle & Fertility Tracker, Healofy Pregnancy & Parenting, Health & Her Menopause App, Know Your Lemons - Self Exam, Me v PMDD, MenoLife. Moody Month: Cycle Tracker, My Calendar - Period Tracker, Natural Cycles, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovulation & Period Tracker, Ovy Partner, Period Calendar Period Tracker, Pregnancy + Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, Stardust, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Garmin Connect™, Kegg, Lovense Remote, Medela Family - Breast Feeding, Oura, Ovy, Tempdrop, We-Vibe, WHOOP
Privacy Policies Mentioning Art 16: *Right to rectification*	**34**	Clover - Safe Period Tracker, Clue period tracker & calendar, FEMM Health and Period Tracker, Flo Period & Ovulation Tracker, Glow Cycle & Fertility Tracker, Healofy Pregnancy & Parenting, Health & Her Menopause App, Know Your Lemons - Self Exam, Me v PMDD, MenoLife. Moody Month: Cycle Tracker, My Calendar - Period Tracker, Natural Cycles, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovulation & Period Tracker, Ovy Partner, Period Calendar Period Tracker, Pregnancy + Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, Stardust, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Garmin Connect™, Kegg, Medela Family - Breast Feeding, Oura, Ovy, Tempdrop We-Vibe WHOOP
Privacy Policies Mentioning Art 17: *Right to erasure ('right to be forgotten')*	**35**	Clover - Safe Period Tracker, Clue period tracker & calendar, FEMM Health and Period Tracker, Flo Period & Ovulation Tracker, Glow Cycle & Fertility Tracker, Healofy Pregnancy & Parenting, Health & Her Menopause App, Know Your Lemons - Self Exam, Me v PMDD, MenoLife. Moody Month: Cycle Tracker, My Calendar - Period Tracker, Natural Cycles, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovulation & Period Tracker, Ovy Partner, Period Calendar Period Tracker, Pregnancy +

[92] Rights of the Individual | European Data Protection Supervisor

[93] Clover - Safe Period Tracker; Flo Period & Ovulation Tracker; Glow Cycle & Fertility Tracker; Health & Her Menopause App; MenoLife - Menopause Tracker; Moody Month: Cycle Tracker; Natural Cycles - Birth Control; Ovulation & Period Tracker; Ovy Partner - Share your Cycle; Pregnancy + | Tracker App; Pregnancy Tracker: amma; Stardust; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Garmin Connect™; Kegg; Medela Family - Breast Feeding; Oura; Ovy; Tempdrop; We-Vibe; WHOOP.

[94] Euki; Frendo Endometriosis Tracker; Kindara Fertility & Ovulation; Oky Period Tracker App; PCOS Tracker; SpotOn; Lioness Health; OvuSense.

		Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, Stardust, Elvie Trainer, Pump with Elvie, Embr Femometer - Fertility Tracker, Garmin Connect™, Kegg, Lovense Remote, Medela Family - Breast Feeding, Oura, OvuSense, Ovy, Tempdrop We-Vibe WHOOP
Privacy Policies Mentioning Art 18: *Right to restriction of processing*	**28**	Clover - Safe Period Tracker, Clue period tracker & calendar, FEMM Health and Period Tracker, Flo Period & Ovulation Tracker, Glow Cycle & Fertility Tracker, Health & Her Menopause App, MenoLife. Moody Month: Cycle Tracker, My Calendar - Period Tracker, Natural Cycles, Ovulation & Period Tracker, Ovy Partner, Pregnancy + Tracker App, Pregnancy Tracker: amma, Stardust, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Garmin Connect™, Kegg, Lovense Remote, Medela Family - Breast Feeding, Oura, Ovy, Tempdrop, We-Vibe, WHOOP
Privacy Policies Mentioning Art 20: *Right to data portability*	**34**	Clover - Safe Period Tracker, Clue period tracker & calendar, FEMM Health and Period Tracker, Flo Period & Ovulation Tracker, Glow Cycle & Fertility Tracker, Health & Her, Know Your Lemons - Self Exam, Me v PMDD, MenoLife, Moody Month: Cycle Tracker, My Calendar - Period Tracker, Natural Cycles, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovulation & Period Tracker, Ovy Partner, Period Calendar Period Tracker, Pregnancy + Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, Stardust, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Garmin Connect™, Kegg, Lovense Remote, Medela Family - Breast Feeding, Oura, Ovy, Tempdrop, We-Vibe, WHOOP
Privacy Policies Mentioning Art 21: *Right to object*	**26**	Clover - Safe Period Tracker, Flo Period & Ovulation Tracker, Glow Cycle & Fertility Tracker, Healofy Pregnancy & Parenting, Health & Her, MenoLife - Menopause Tracker, Moody Month: Cycle Tracker, Natural Cycles - Birth Control, Ovulation & Period Tracker, Ovy Partner, Period Calendar Period Tracker, Pregnancy + Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, Stardust, Elvie Trainer, Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Garmin Connect™, Kegg, Medela Family - Breast Feeding, Oura, Ovy, Tempdrop, We-Vibe, WHOOP
Of the 36 policies which include *at least some* rights:		
Policies Explaining these Rights (as opposed to merely listing them) *	**18**	Clue period tracker & calendar; Flo Period & Ovulation Tracker; Glow Cycle & Fertility Tracker; Me v PMDD; MenoLife - Menopause Tracker;; Ovulation & Period Tracker; Period Calendar Period Tracker; Pregnancy App & Baby Tracker; Stardust; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Garmin Connect™; Kegg; Lovense Remote; Oura; Tempdrop; WHOOP
Policies Detailing How to Exercise Rights	**31**	Clue period tracker & calendar; FEMM Health and Period Tracker, Flo Period & Ovulation Tracker; Glow Cycle & Fertility Tracker; Healofy Pregnancy & Parenting Health & Her Menopause App; Me v PMDD; MenoLife - Menopause Tracker; Moody Month: Cycle Tracker; Natural Cycles - Birth Control; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy & Baby Tracker; Ovy Partner - Share your Cycle; Period Calendar Period Tracker; Pregnancy + | Tracker App; Pregnancy App & Baby Tracker; Pregnancy Tracker: amma; Stardust; Elvie Trainer; Pump with Elvie; Embr Wave 2: Hot Flash Relief; Femometer - Fertility Tracker; Garmin Connect™; Kegg; Lovense Remote; Medela Family - Breast Feeding; Oura; Ovy; Tempdrop; We-Vibe; WHOOP

Certain policies which mentioned (some) data subject rights did so without explicitly linking them to, or even mentioning, the GDPR: e.g. FEMM Health & Period Tracker, Know Your Lemons, and Healofy Pregnancy & Parenting. While this might make it harder for users to understand or identify the relevant legal framework (and thus, potentially, the mechanisms for

taking action), we do not consider failure to explicitly link the rights to the GDPR an issue of non-compliance *per se.*

16. AI Processing

14 of 42 apps included in our survey mentioned artificial intelligence (AI) / automated or algorithmic processing / machine learning in the Privacy Policies and / or Terms of Use. This is detailed below:

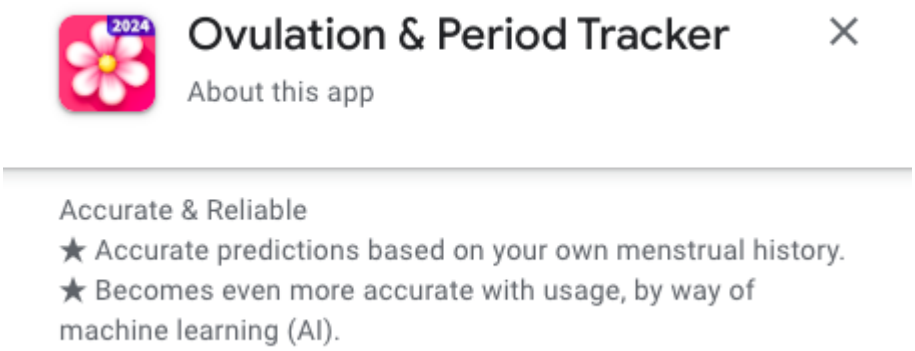
App	Policy Claims / Disclaims Use of Automated Tools	Additional Details
Clover - Safe Period Tracker	Claims	User data may be used "to help understand your needs and provide you with better service (to use in the training of neural networks, artificial intelligence, as well as for any other automated decision-making processing)"
Clue period tracker & calendar	Claims	"Statistical and algorithmic data processing" is used to identify patterns in a user's menstrual cycles or pregnancy. Users' data is also used to "develop new algorithms". However, Clue specifies that it "does not engage in any automated decision-making or profiling activities."
Flo Period & Ovulation Tracker	Partially Claims	Tecton Inc (a 'Machine Learning Development Platform')
Glow Cycle & Fertility Tracker	Partially disclaims	"We are not making automated decisions about you. We may use profiling in regard to your personal information required to operate some of our services, for example, to the extent needed to predict health-related effects that you may experience from one month to the other."
Natural Cycles - Birth Control	Claims	"Natural Cycles uses an algorithm that is sensitive to subtle patterns in a woman's cycle to determine her daily fertility"
Ovia: Fertility, Cycle, Health	Claims	"Ovia Health's proprietary health algorithms analyze users' data and provide customized content in return, with the goal that users will achieve better health outcomes due to the content Ovia has provided. For example, users may track their menstrual periods, symptoms, and weight to receive feedback on when they are most fertile. The Services are educational only and provide no guarantee that users will accomplish any of their reproductive health goals."
Ovia: Pregnancy & Baby Tracker	Claims	"Ovia Health's proprietary health algorithms analyze users' data and provide customized content in return, with the goal that users will achieve better health outcomes due to the content Ovia has provided. For example, users may track their menstrual periods, symptoms, and weight to receive feedback on when they are most fertile. The Services are educational only and provide no guarantee that users will accomplish any of their reproductive health goals."
Ovy Partner - Share your Cycle	Claims	"An algorithm calculates the user's menstrual cycle and curve. The more information is entered into the app, the better the predictions will be."
Pregnancy Tracker: amma	Claims	"We process your personal data by automated means, including in information and telecommunication networks and/or without them."
		"We use intelligent algorithms that provide certain App functions, such as

Femometer - Fertility Tracker	Claims	predictions of your cycle and ovulation day. The more Personal Data about your cycle, ovulation tests, and BBT that our intelligence algorithm can work with, the better predictions you get from the algorithm."
Garmin Connect™	Partially disclaims	"We do not make any decisions based on algorithms or other automated processing that significantly affect you."
Lovense Remote	Claims	"Lovense may provide AI-powered service or function ("AI service") by using technology provided by third-party service providers ("AI Provider")". Note: it specifically disclaims "accuracy, completeness or applicability" of the information generated.
Ovy BBT	Claims	"An algorithm calculates the user's menstrual cycle and curve. The more information is entered into the app, the better the predictions will be."
WHOOP	Claims	Only for operating and training the WHOOP Coach (Generative AI) Function.[95]

In some instances, the algorithmic tools were given a misleading lack of prominence and could easily be missed by users. For example, Flo's website described the app as an "*AI-powered health app that supports women during their entire reproductive lives – from first menstruation to menopause*",[96] which "*uses a set of complex [AI-driven] algorithms to make predictions*."[97] However, only a brief and oblique mention was made to this fact in the Privacy Policy – which referred to Tecton Inc (a 'Machine Learning Development Platform').

There are also a number of apps (Lioness, Moody Month, Oky, Ovulation & Period Tracker, Oky and Tempdrop) which did make use of such tools, but this was not mentioned explicitly in their Privacy Policies or Terms of Use at all.[98] For example, on Google Play Store, the description for Moody Month reads "*Moody Month is a cycle tracker that uses AI to track daily hormone changes, spot patterns and offer solutions that support your mental and physical health.*" However, there is no mention of this in the privacy policy or the terms of use. Another such example is Ovulation & Period Tracker: there was no mention of AI / automated or algorithmic processing / machine learning in the associated policies, but the Play Store description included the following:

[95] WHOOP, 'Introducing WHOOP Coach, Powered By OpenAI' (26 September 2023) <https://www.whoop.com/gb/en/thelocker/introducing-whoop-coach-powered-by-openai/> accessed 9th September 2024.
[96] Flo, 'What is Flo?' <https://help.flo.health/hc/en-us/articles/4406825500052-What-is-Flo> accessed: 9th September 2024.
[97] Flo, 'Glossary, <https://help.flo.health/hc/en-us/articles/4406826083860-Flo-glossary> accessed: 9th September 2024.
[98] We identified these by looking at the website and marketing of the apps, their descriptions on the Play Store and by downloading the apps themselves.



The GDPR defines 'profiling' as:

> 'Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.'[99]

It further provides data subjects with a right not to be subject to a decision 'based solely on automated processing, including profiling', which produces legal effects concerning them or similarly significantly affects them.[100]

Femtech apps normally market themselves as offering algorithmic- driven predictions on future gynaecological conditions, such as predicting future menstrual and ovulation periods. Most apps / wearables surveyed did not explicitly mention the term 'profiling', but mentioned automatically collecting data about users' online activity, often via the use of cookies or by combining data about a user from several different sources, and automated decision-making.

Of the five apps that mentioned profiling specifically, Clue stressed that they did not engage in profiling: "*Clue does not engage in any automated decision-making or profiling activities*".

Glow was the only app to explicitly state that they engage in profiling:

> "*We may use profiling in regard to your personal information required to operate some of our services, for example, to the extent needed to predict health-related effects that you may experience from one month to the other. You can object to such profiling by contacting us at support@glowing.com.*"

[99] Art. 4(4) GDPR.
[100] Art. 22 (1) GDPR. The second paragraph of the same Article provides that 'Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;… or (c) is based on the data subject's explicit consent.' Paragraph 3 states that 'In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.'

Others mentioned the users' right to opt out of profiling. For example, MenoLife stated: *"[you have the right to] opt out of the processing of your personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning you.*" They went on to state the effects of a user opting out:

> *"In any case, we will not increase the cost of, or decrease the availability of, a product or service, based solely on the exercise of any of your rights and unrelated to the feasibility or the value of a service. However, to the extent permitted by the law, we may offer a different price, rate, level, quality, or selection of goods or services to you, including offering goods or services for no fee, if our offer is related to your voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program."*

While it is not specified, this leaves it open that users who do not consent to profiling may receive a poorer quality of service - in the context of period tracking, this could potentially mean receiving less accurate predictions.

Stardust stated in the data subject rights section of the privacy policy that users have "*the right to not be subject to a decision based solely on automated decision making, including profiling, where the decision would have a legal effect on you or produce a similarly significant effect*." No further detail was provided about the eventuality of such decisions besides repeating the GDPR's pronouncement.

SpotOn stated that: "*We do not engage in profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer*."

Regarding automated decision making, Garmin stated that "*We do not make any decisions based on algorithms or other automated processing that significantly affect you*". However, no further clarification was provided as to what such decisions might entail and what is excluded from these decisions.

Automated decision making was also mentioned by Clover:

> "*We may use your personal information...to link or combine with information we get from others (except data from Apple HealthKit, Core Motion Framework, and Google Fit) or (and) from you to help understand your needs and provide you with better service (to use in the training of neural networks, artificial intelligence, as well a for any other automated decision-making processing)"*

Overall, it is concerning that the research found little mention of any specific guarantees applicable when AI is used to analyse women's sexual and reproductive data and generate relevant predictions.

17. Data Security

Data security—protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures—is crucial in the context of femtech. Our research surveyed the following: whether the privacy policies mention data security; whether users' data that femtech collects is stored locally or remotely, on a server; whether the policies mention encryption; and whether data controllers/ processors of such data have carried out any risk / impact assessments regarding the severity of the harm that could result from this data not being fully secure. The Table summarises the findings, followed by a discussion of their implications.

Data Security (apps and wearables)

	Yes	**No**	**Only partially**	**Not mentioned/ N/A /Not clear**
Does the app/ wearable explicitly mention data security?	**25** Clover; Clue; FEMM; Flo; Glow; Healofy; Health and Her; Kindara; Know Your Lemons; Me v PMDD; Moody Month; MenoLife; My Calendar Period Tracker; Natural Cycles; Oky; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy and Baby Tracker; Ovulation and Period Tracker; PCOS; Period Tracker Period Calendar; Pregnancy + | Tracker App Pregnancy App and Baby Tracker; Pregnancy Tracker: amma; Spot On; Stardust; **8**	**2** Frendo; Ovy **6** Femometer; Oura[101] Ovy; Tempdrop; We-Vibe; Whoop		1 Garmin Lily - 'smart watch for women'

[101] As noted below, in the section on data security, Femometer and Oura Ring are included in this section because, though they do *mention* data security, they do so only in regard to what the *user* can do to keep their data safe: "Information Security: We believe that the largest threat to security and privacy is that someone could get your device and account information. You can help keep your Personal Information secure by properly selecting and protecting passwords, not sharing passwords with others, and preventing others from using your mobile device, laptop or other devices that can access the Services." From Femometer Privacy Policy, section titled 'information security'. Available at: https://www.femometer.com/de/PrivacyPolicy?srsltid=AfmBOorgf_X0FI13YzkxfwNNFL2Ee2fbJaXQd1mflwzwfXLtmYkRmgKI.
"We update our Products regularly to protect your personal data. We recommend that you make sure that you always have the latest app and firmware versions installed in order to maximize protection of your data." From Oura Privacy Policy. Available at: https://ouraring.com/privacy-policy?srsltid=AfmBOoombzAQfjc_nhxGbiZhcu4r3Ddvrx5TTF1611DOHz7xeWZzutS6.

	Elvie Smart Trainer and Breast Pump; Embr WristBand; Kegg Fertility Tracker; Lioness Smart Vibrator; Lovense Smart Vibrator; Medela Smart Breast Pump; Lioness Smart Vibrator; Lovense Smart Vibrator; OvuSense Fertility Monitor			
Is data only stored locally in the device?	**2** My Calendar; Ovulation;	**22** Clover; Clue; FEMM; Flo; Frendo; Glow; Healofy; Health and Her; Kindara; Me v PMDD; MenoLife; Moody Month; Natural Cycles; Ovia: Fertility, Cycle, Health; Ovia: Pregnancy and Baby Tracker; Ovy; PCOS; Pregnancy + | Tracker App; Pregnancy App and Baby Tracker; Pregnancy Tracker: amma; Spot on; Stardust 14 Elvie Trainer; Elvie Breast Pump; Embr Wave; Garmin Lily; kegg; Lioness Health; Lovense; Medela; Oura; OvuSense; Ovy; TempDrop; WeVibe; WHOOP	**3** Know your Lemons; Oky Period Tracker; Period Tracker, Period Calendar	Euki doesn't collect or store personal information Amma Pregnancy and Baby Tracker doesn't collect any data 1 Femometer
Is encryption mentioned?	**13** FEMM; Flo; Kindara; Me v PMDD; Moody Month; My Calendar; Natural Cycles; Ovia: Pregnancy and Baby Tracker; Ovia: Pregnancy and Baby Tracker; Pregnancy App & Baby Tracker PCOS; Spot On; Stardust **4** Elvie Smart Trainer; kegg Fertility Tracker; Lovense Smart Vibrator; Oura Ring	**13** Clover; Clue; Frendo; Glow; Healofy; Health and Her; Know Your Lemons; Oky; Ovulation and Period Tracker; Ovy; MenoLife; Period Calendar, Period Tracker; Pregnancy + | Tracker App; **11** Elvie Breast Pump; Embr WristBand; Femometer; Garmin Lily - 'Smart Watch for Women'; Lioness Smart Vibrator; Medela; OvuSense;	**1** Pregnancy Tracker: amma	

		Ovy; Tempdrop; We Vibe[102]; WHOOP		

The study found that not a single app or wearable could guarantee the complete security of the user's data, and many made explicit disclaimers about this- e.g. "*Despite FEMM's efforts to protect your Personally Identifiable Information and Personal Health Information, there is always some risk that an unauthorized third party may find a way around our security systems or that transmissions of your information over the Internet may be intercepted*."[103] Oky noted: "*We use many reasonable measures – physical and electronic – to prevent unauthorized access and disclosure of your data. However, it is always a possibility that third parties may unlawfully intercept or access your data. So, although we work extremely hard to safeguard your data, we cannot guarantee that your data will always remain private*."[104] Likewise, after making clear what it does to protect user's privacy, Moody Month stated: "*You should be aware, however, that the transmission of information via the Internet is not completely secure*."[105]

Other policies emphasised what they did to keep user data safe: For example, Know Your Lemons, mentioned "*To ensure the security and confidentiality of personal data collected online, we use data networks protected, inter alia, by industry standard firewall and password protection. In the course of handling your personal data, we take measures reasonably designed to protect such data from loss, misuse, unauthorized access, disclosure, alteration or destruction*."[106] Similarly, Natural Cycles stated that "*We use generally accepted industry standards, technologies, procedures and methods, such as firewalls, encrypted storage, pseudonymization, regular software updates, security scans, access control, audit logging and review of admin actions as well as external penetration tests to protect the integrity of your Personal Data and to prevent unauthorized access*."[107]

What is notable here is that the absence of a disclaimer did not mean these apps / wearables were claiming to keep user data completely secure. Phrases such as "industry standards" or "industry best practices"[108] were often found to be employed in this context (e.g. "*Kindara and its web hosting contractors takes every reasonable effort, employing all industry-standard*

[102] We-Vibe's privacy policy mentions encryption twice, but very briefly and without elaboration: "Encrypted communication content exchanged with other users via the app" and "Twilio provides communication services to enable you to have encrypted audio and video chats" from We-Vibe Privacy Policy. Available at: https://www.we-vibe.com/us/privacy-policy.
[103] FEMM Privacy Policy, Section 7. Available at: https://femmhealth.org/privacy-policy/#:~:text=The%20FEMM%20App%20uses%20data,view%2C%20or%20share%20your%20information.
[104] Oky Privacy Policy. Available at: https://okyapp.info/privacy-policy/#:~:text=We%20collect%20information%20on%20the,they%20are%20engaging%20with%20Oky.
[105] Moody Month Privacy Policy, Section 9. Available at: https://moodymonth.com/privacy-statement.
[106] Know Your Lemons Privacy Policy, section titled 'Security and Confidentiality'. Available at: https://www.knowyourlemons.org/privacy-policy.
[107] Natural Cycles Privacy Policy, Section 7. Available at: https://www.naturalcycles.com/other/legal/privacy.
[108] These phrases were used by 11 apps / wearables.

practices to keep your information safe"[109]). However, if industry standards are insufficient, data security cannot be guaranteed.

Further, sometimes these disclaimers used language that shifted the burden of responsibility away from the company. As Femometer stated "*You can help keep your Personal Information secure by properly selecting and protecting passwords, not sharing passwords with others, and preventing others from using your mobile device, laptop or other devices that can access the Services*"[110].

Notably, this implied shifting of responsibility was repeated in Femometer's Terms of Use: "*Femometer uses industry-standard security measures to protect the loss, misuse and alteration of the information under our control. Although we make good faith efforts to store the non-public information uploaded through the Services or collected by Femometer in a secure operating environment that is not available to the public, we cannot guarantee complete security. We cannot and do not guarantee that our security measures will prevent third party "hackers" from illegally accessing our site and obtaining access to content or information thereon.*"[111]

As the table shows, the vast majority of apps stored user data remotely, on a server rather than on the user's device. However, there were a few exceptions to this. My Calendar - Period Tracker, Ovulation and Period Tracker, and Periodical all stored their data locally, with the option of the user backing this data up remotely (e.g. on the cloud) if they chose[112]. Others specified that some data was stored locally while other data was stored remotely. For example, health information was only stored locally for two apps (Period Calendar Period Tracker, Know Your Lemons - Self-exam[113]); similarly, Oky Period Tracking App stored information the user inputs on their 'day card' - such as body, mood, activity and flow, and their daily diary card - locally, while storing the rest on servers.[114] Pregnancy Tracker: amma stored everything remotely except the calendar function.[115] The remaining apps stored everything remotely. As

[109] Kindara Privacy Policy. Section titled 'Security'. Available at: https://www.kindara.com/privacy-policy#:~:text=Kindara%20collects%20and%20uses%20the,health%2Drelated%20information%20you%20provide.

[110] Femometer Privacy Policy, section titled 'information security'. Available at: https://www.femometer.com/de/PrivacyPolicy?srsltid=AfmBOorgf_X0FI13YzkxfwNNFL2Ee2fbJaXQd1mflwzwfXLtmYkRmgKI.

[111] From Femometer's Terms of Use, Section titled Your Privacy and the Use of Your Data. Available at: https://www.femometer.com/de/TC.

[112] My Calendar - Period Tracker Privacy Policy. Available at: https://simpleinnovation.us/my-calendar/privacy-policy.
Ovulation and Period Tracker Privacy Policy. Available at: https://leap.app/privacypolicy.html?pkg=periodtracker.pregnancy.ovulationtracker.
Periodical only provides a (local to device) calendar, which does not collect any data and does not require a user registration.

[113] Period Calendar Period Tracker Privacy Policy. Available at: https://simpledesign.ltd/privacy/my_calendar.html.
Know Your Lemons - Self-exam Privacy Policy. Available at: https://www.knowyourlemons.org/privacy-policy#:~:text=We%20only%20store%20your%20email,any%20email%20we%20send%20you.

[114]Oky Privacy Policy, Section 2. Available at: https://okyapp.info/privacy-policy/#:~:text=We%20collect%20information%20on%20the,they%20are%20engaging%20with%20Oky.

[115] Pregnancy Tracker: amma Privacy Policy.

expected, all the wearables studied stored data remotely, normally on the accompanying device on which the app is used.

In terms of encryption,[116] the picture was highly variable. 13 apps and 8 wearables did not mention encryption in their privacy policy. Among those that did, there was much variation regarding what kinds of data were encrypted, and some were more detailed regarding this than others. For instance, Ovia stated that it "*protects personal data with security measures that are consistent with industry standards, including...data encryption in transit and at rest*."[117]

Me v PMDD outlined a number of steps taken to keep user data safe:

> "*When you use Me v PMDD, your personal profile data is stored separately from your symptom and treatment tracking data and your service settings. This ensures a high level of privacy for your tracking information. Your password is stored using one-way encryption ("hashing" plus "salting"), and it cannot be read by us. We use HTTPS protocol to encrypt your data when it is transmitted between your device and Me v PMDD's servers. HTTPS is also the same technology that ensures secure connections in your web browser indicated by a padlock icon.*"[118]

There was also a difference between whether and how encryption was specified in the privacy policies, and how it was presented in the Google Play Store. 16 apps / wearables stated in a "data safety" notice on the Google Play Store that the data they processed was "encrypted in transit"[119], but their privacy policy did not mention encryption at all, or left it unclear as to what data exactly was and was not encrypted (another stated in the "data safety" notice that data "was not encrypted during transit")[120].

18. Community groups

It is worth noting that a number of apps offer community chats where users with similar interests can share information and support one another. For instance, Glow offers several community groups including 'Sex & Relationships', 'Health & Lifestyle', 'Period Talk', 'Birth Control', 'Adult Relationships', 'Am I Pregnant?', 'Glow Gift Exchange', 'Controversy Corner', 'Fitness & Exercise', 'Sports & Games', 'Love', 'Beauty', 'Self Care', 'FemCare Product Reviews'. Glow's policy stated that "*You are free to make sensitive information public on the Community Forum (such as your political opinions and religious beliefs) but remember that this information is visible to other users*."

[116] Please see also 'Femtech Traffic Analysis Research Report'.
[117] Ovia Privacy Policy. Available at: https://www.oviahealth.com/privacy-policy/
[118] Me v PMDD Privacy Policy. Available at https://mevpmdd.zendesk.com/hc/en-us/articles/115002446311-Privacy-Policy.
[119] Clover, Frendo, Glow, Healofy, Health and Her, My Calendar, Oky, Ovulation and Period Tracker, Period Calendar Period Tracker, Pregnancy + | Tracker App Pregnancy Tracker: amma, Elvie Pelvic Floor Trainer, Garmin Lily, Lioness Smart Vibrator, Medela Smart Breast Pump, Tempdrop Armband.
[120] Femometer App. Data notice available on the Google Play Store webpage: https://play.google.com/store/apps/details?id=com.bm.android.thermometer&hl=en_GB.

Flo's policy mentioned that "*the App features several community areas like Secret Chats… Any information (including personal data) you share in any online community area or online discussion is by design open to the Flo community. Please think carefully before posting any personal data in any public forum. What you post can be seen, disclosed to, or collected by others and may be used in ways we cannot control or predict, including to contact you for unauthorized purposes. Posting your personal data in Secret Chats will violate the Secret Chats Rules*."

Similarly, FEMM noted that it:

"*features public areas where users with similar interests or medical conditions can share information and support one another or where users can post questions for experts to answer. Our public areas are open to the public and should not be considered private.*
Any information you share in any online community area (including Personally Identifiable and Personal Health Information) like a chat room, forum posting, or online discussion is by design open to the public and is not private. You should think carefully before posting any Personally Identifiable or Personal Health Information in any public forum. What you post can be seen, disclosed to or collected by third parties and may be used by others in ways we cannot control or predict, including to contact you for unauthorized purposes. As with any public forum on any site, the information you post may also show up in third-party search engines like Google, Yahoo, MSN, Bing, etc."

Community chats are also available in the case of femtech wearables. For example, Medela's policy stated that "*you can… ask questions and share knowledge with one another on our "Mums Community" platform ("Community"). We do not request or process any personal data for the Community. However, by participating in our Community you can voluntarily disclose such data to Medela. By accepting our rules and entering such personal data you consent to the processing of such data by Medela. You can withdraw your consent at any time by deleting the respective data or by deleting the App. This will not affect the lawfulness of the data processing according to your consent given prior to the withdrawal*."

The Lioness' policy mentioned that "*The Lioness Service may offer discussion forums, message boards, social networking opportunities, chat pages and other public forums or features in which you may provide personal information, materials and related content. If you submit personal information when using these public features, please note that such personal information may be publicly posted and otherwise disclosed and used without limitation or restriction.*"

Interestingly, Ovia mentioned that "*If you opt-out of marketing emails and push notifications, you will still receive account management notices. To stop all emails and push notifications, you must delete your account and data. If we delete your data, we will not delete the posts or comments you have shared publicly on Ovia's social media, community or chat features*."

19. Data Protection Impact Assessments (DPIAs)

Of the policies we surveyed, only two made explicit mention of Data Protection Impact Assessments (DPIAs),[121] though neither provided specific details about where these could be found. For instance, Flo mentioned that they conducted *"periodical data protection impact assessments in order to ensure that the Services fully adhere to the principles of privacy by design, privacy by default, and others. We also commit to undertake a privacy audit in the event of Flo's merger or takeover*."[122]

We consider DPIAs crucial in the femtech context. It is, therefore, regrettable that so few policies explicitly referred to them. Ideally, such DPIAs should seek the engagement of data subjects in this context.[123]

20. Data Protection Officers (DPOs)

20 of the 42 policies mentioned a Data Protection Officer (DPO),[124] and provided information about how to contact them specifically. DPOs monitor data controllers' compliance with the GDPR and are, therefore, very important in this context.

21. Right to Lodge a Complaint

27 of 42 policies mentioned specifically that the user has the right to lodge a complaint with a supervisory authority / data protection authority.[125] This was dealt with varying levels of detail and specificity across the policies. For example, the TempDrop policy provided fairly detailed information regarding this right: "*Subject to applicable law, you have the right to lodge a complaint with your local data protection authority. If you are in the EU, you can lodge a complaint to the supervisory authority, in particular in the Member State of your residence, place of work or of an alleged infringement of the GDPR. For a list of supervisory authorities in the EU, click here* [LINK]*."* Other policies merely stated that users had the right to lodge a complaint with the relevant supervisory / data protection authority, without providing any further information.[126]

[121] Article 35 GDPR.
[122] WHOOP mentioned that it undertakes regular cyber- security impact assessment.
[123] Art. 35(9) GDPR.
[124] Additionally, one policy (Healofy) refers to a 'Grievance Officer'.
[125] Clue period tracker & calendar, Flo Period & Ovulation Tracker, Frendo Endometriosis Tracker, Glow Cycle & Fertility Tracker, Health & Her Menopause App, Know Your Lemons - Self Exam, MenoLife - Menopause Tracker, Moody Month: Cycle Tracker, My Calendar - Period Tracker, Natural Cycles - Birth Control, Ovia: Fertility, Cycle, Health, Ovia: Pregnancy & Baby Tracker, Ovy Partner - Share your Cycle, Period Calendar Period Tracker, Pregnancy + | Tracker App, Pregnancy App & Baby Tracker, Pregnancy Tracker: amma, Elvie Trainer , Pump with Elvie, Embr Wave 2: Hot Flash Relief, Femometer - Fertility Tracker, Garmin Connect™, Oura, Ovy, Tempdrop, We-Vibe, WHOOP
[126] For example, My Calendar - Period Tracker provided that EU users "*may always lodge a complaint with a supervisory authority*"; Ovy pointed that, "*As a data subjects*", users have the right to "*lodge a complaint with the competent supervisory authority regarding unlawful data processing*"; Garmin Connect™ privacy policy

Four of the Privacy Policies (Flo, Natural Cycles , Pregnancy App & Baby Tracker, and WHOOP) contained additional statements about the right to access arbitration procedures regarding specific data protection matters. For instance, Flo's Privacy Policy stated: *"You may also be able to invoke binding arbitration for unresolved complaints, but prior to initiating such arbitration, a resident of a European country (including Switzerland) participating in the DPF must first (1) contact us and afford us the opportunity to resolve the issue; (2) seek assistance from JAMS; and (3) contact the US Department of Commerce (either directly or through a European data protection authority) and afford the Department of Commerce time to attempt to resolve the issue."*

22. Data Transfers

31 of 42 apps stated that data *is or may be* transferred to a non-EU country (included in this list are apps where the policies indicated that data may be transferred or maintained outside of the user's state / country / jurisdiction, even if they did not specifically mention the EU).

15 of the privacy policies made reference to the GDPR transfer of personal data to third countries provisions (GDPR, Chapter V).[127] A couple were more ambiguous, referring to protection of transferred data in more general terms:

- **Oura:** "*We use industry standard data protection measures to safeguard all international transfers of personal data through data protection agreements with our service providers*".

- **Embr Wave 2:** Hot Flash Relief "*Our contracts with our service providers ensure that they use appropriate safeguards to transfer your Personal Information to the United States.*"

- **Period Calendar Period Tracker:** "*no transfer of your information will take place to an organization or a country unless there are adequate controls in place*."

Seven apps specifically mentioned the EU-US / Swiss-US Data Privacy Framework[128] when discussing the transfer of data to the US.[129]

directed readers to a separate page (entitled, 'Your Data Protection Rights') where the right to lodge a complaint was set out: "*You have the right to…lodge a complaint with a supervisory authority.*"

[127] Transfers of personal data to a third country may take place on an adequacy decision (Art. 45 GDPR), subject to appropriate safeguards (Art. 46 GDPR) and on Binding Corporate Rules (Art. 47 GDPR).

[128] Data Privacy Framework Programme, 'Data Privacy Framework (DPF) Program Overview' <https://www.dataprivacyframework.gov/Program-Overview#:~:text=The%20EU%2DU.S.%20Data%20Privacy,with%20reliable%20mechanisms%20for%20personal> accessed: 19th September 2024.

[129] Clue period tracker & calendar, Flo Period & Ovulation Tracker, Moody Month: Cycle Tracker, Natural Cycles - Birth Control, Pregnancy App & Baby Tracker, Garmin Connect™, WHOOP. WHOOP stated that they no longer 'rely' on these frameworks to facilitate cross-border transfers, but remain committed to their principles nonetheless.

It is worth noting that in 2019, the Federal Trade Commission lodged a complaint against Flo, alleging - amongst other things - that Flo violated the EU-U.S. and Swiss-U.S. Privacy Shield framework. A settlement was reached in 2021.[130] Currently, Flo's policy provides that "*When transferring personal data outside the EU, EEA, and UK, we either implement standard contractual clauses, conduct transfer impact assessments, or rely on current European Commission adequacy decisions*."

23. Terms of Service documents

In addition to Privacy Policies, most femtech apps / wearables provided a Terms of Service / Terms of Use/ Terms and Conditions document, which focused on a given company's legal obligations (or lack thereof) to users regarding their engagement with the app / wearable. The Table below details the different disclaimers contained therein.

[130] Federal Trade Commission 'FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others' (22 June 2021) <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google> accessed: 19th September 2024.

Apps	Warranty Disclaimed	Exclusion of Liability	Mentioned Contractual Liability?	Jurisdiction	Incorporates Privacy Policy?
Clover	Does not guarantee: accuracy; suitability for international use; Disclaimed to the fullest extent permitted by law	Not liable; damages limited to $50	Not mentioned	Laws of the Republic of Cyprus	Mentioned but not incorporated
Clue	Not medical advice; Use at your own risk; No guarantee of disruption free use; No guarantee of functionality	Liable for foreseeable damages in specific cases	Not mentioned	Germany	Mentioned but incorporation not explicitly explained
Drip	Does not collect personal data	Not mentioned	Not mentioned	Not mentioned	Not mentioned
Euki	Does not collect personal data	Not mentioned	Not mentioned	Not mentioned	Not mentioned
FEMM	Not medical advice; Disclaimed to the fullest extent permitted by law	Not liable. Can only be found liable for actual damages, this cannot exceed $1000	Not liable for any damages, based on any theory of law	State of New York	Incorporated: T&Cs prevail in case of conflict
Flo	Not medical advice; Use by minors; Not responsible for third-party information; Disclaimed to the fullest extent permitted by law	Not liable. If found liable, total amount of damages cannot exceed amount paid to app or $100	Excluded where permitted by law	If US resident: Delaware or the State where the complainant resides. If EU, UK, Switzerland, Norway or Iceland resident: the court of residence.	Agreeing to T&Cs = agreeing to Privacy Policy
Frendo	Not medical advice; no doctor-patient relationship; Disclaimed to the fullest extent permitted by law	Not liable. If found liable, total amount of damages cannot exceed amount paid to app or $100	Not mentioned	Not mentioned	Not mentioned
Glow	Not medical advice; Not liable for accuracy of third party information; Fully disclaimed	Not liable. If found liable, total amount of damages cannot exceed amount paid to app or $100	Not liable for any damages, based on any theory of law	State of Delaware	Agreeing to T&Cs = agreeing to Privacy Policy
Healofy	Not medical, counselling, legal or other professional advice; Does not guarantee the service will be accurate/ complete /timely; Fully disclaimed	Not liable for any damages	Not liable for any damages, based on any theory of law	Not mentioned	Privacy policy forms part of overall agreement
Health and Her	Not medical advice; Not for	Liable for foreseeable	If part of the contract is	English, Scottish or	Privacy policy states that it does not

Menopause	minors: Not responsible for third-party content; Information not fully up to date or accurate	loss or damage caused; Liable for property damage; Not liable for business loses	found illegal, the rest will continue in force; If they delay in enforcing contract, they can still enforce it later	Northern Irish courts	override or replace T&Cs
Kindara	Not medical advice; Not responsible for risks of sexual activity/ pregnancy; Not responsible for third-party content; Disclaimed to the fullest extent permitted by law	To the fullest extent permitted by law	Not liable for any damages, based on any theory of law	State of Colorado	States that they are incorporated
Know Your Lemons	Not medical advice; Cannot guarantee accuracy	Not liable	Not mentioned	Not mentioned	Only one document: the privacy policy
Me v PMDD	Not medical advice	Not liable if services provided are used against explicit instructions (e.g. as medical advice) Damages limited to amount paid for app	Not mentioned	Not mentioned	Mentioned but not incorporated
MenoLife	Used at own risk; Cannot guarantee accuracy; Not medical advice; Disclaimed to the extent permitted by law	Not mentioned	Not mentioned	Arizona	Mentioned but not incorporated
Moody Month	Services will not always be accurate/ timely/ fully functional/ secure/ compatible with device; Disclaimed to the extent permitted by law	Not liable to the extent permitted by law	Will not be liable in contract; Not liable for contracts made with third party suppliers	England and Wales; Non-exclusive jurisdiction	Agreeing to the terms implies agreeing to the privacy policy
My Calendar	No terms of service				
Natural Cycles Birth Control	Information will not be fully accurate; Services may not be clinically effective for women under 18; Not medical advice; Use at own risk	Not liable to the extent permitted by law; Damages cannot exceed total payments to app	No liability based in contract	Sweden	Privacy policy considered part of terms of service
Oky Fertility	The service is not medical advice or a contraceptive;	Not liable to the extent permitted by	Liability only mentioned with regard to	Not mentioned	Privacy policy mentioned but not incorporated

	will not run uninterrupted; will not guarantee pregnancy; will not always be accurate	law	third parties - not liable for third party information		
Oky Pregnancy	Same as above	Not mentioned	Not mentioned	Not mentioned	Not mentioned
Ovulation and period tracker	No terms of service	Not mentioned	Not mentioned	Not mentioned	Not mentioned
PCOS Tracker	No terms of service - but the 'learn more' section of the app states that it does not provide medical advice	Not mentioned	Not mentioned	Not mentioned	Not mentioned
Period Calendar Period Tracker	No terms of service	Not mentioned	Not mentioned	Not mentioned	Not mentioned-
Pregnancy + | Tracker App	Not medical advice; Not responsible for third-party links/ information; Fully disclaimed	Not liable to the extent permitted by law	Not liable under any contract	State of New York	Agreeing to the terms implies agreeing to the privacy policy
Pregnancy Tracker: amma	Not medical advice; not for use by minors; not responsible for third-party content; can't guarantee accuracy of algorithmic data	Not liable to the extent permitted by law	Not mentioned	United Mexican States	Mentioned but not incorporated
Spot On	Not a healthcare service; Not responsible for third party links	Not liable to the fullest extent permitted by law	Not mentioned	State of New York	Privacy policy incorporated into terms of service
Stardust	Not medical advice; Not responsible for third-party links	Not liable to the fullest extent permitted by law. Liable only for up to 6 months of subscription fee or $500	Not liable under any contract	State of New York	Mentioned but not incorporated
Elvie	Not medical advice; Not responsible for third-party content; not responsible for user-created content; Cannot guarantee accuracy, uninterrupted service or functionality	Not liable to the fullest extent permitted by law	Any product offered does not amount to a legally-binding contract	Laws of England and Wales, exclusive jurisdiction	Privacy policy forms part of the overall agreement
Embr	Cannot guarantee accuracy,	Not liable to the fullest	Not liable under any	The laws of the Commonwealth	Incorporated

	uninterrupted service, functionality, protection from computer viruses, suitability outside the US; not responsible for third-parties	extent permitted by law	contract	of Massachusetts	
Femometer	Not medical advice; Not for users under 18; Cannot guarantee data security	Not liable to the fullest extent permitted by law	Not liable under any theory of law	Not mentioned	Mentioned but not incorporated
Garmin Lily	Cannot guarantee accuracy; Not medical advice; Not responsible for user content; Not responsible for third-party services/products	Not liable to the fullest extent permitted by law	Not liable under any contract	State of Kansas	Not mentioned
kegg Fertility	No guarantee the wearable/service is permitted in user's jurisdiction, that it will be accurate, guarantee pregnancy, that service will be uninterrupted; Not responsible for third-parties; Not medical advice **Warranty offered: 1 month money-back guarantee; 1 year guarantee against defectiveness**	Not liable to the fullest extent permitted by law	Not liable under any contract	State of California	Privacy policy forms part of the overall agreement
Lioness	No guarantee of uninterrupted service, accuracy, timeliness, safety of service; Use at own risk; Not medical advice; User responsible for keeping account details private	Not liable to the fullest extent permitted by law	Not liable under any contract	State of California	Privacy policy forms part of the overall agreement
Lovense	No guarantee of uninterrupted service, accuracy, timeliness, safety of service; Use at own risk; Not medical advice	Not liable to the fullest extent permitted by law	Not mentioned	Laws of Hong Kong	Privacy policy forms part of the overall agreement
Medela	No terms of service	N/A	N/A	N/A	N/A

Oura	No responsibility for data damage or loss; Not medical advice; Not responsible for third party content; **Warranty offered: 1 year guarantee against defectiveness**	Not liable to the fullest extent permitted by law	Not liable under any contract	Laws of Finland	Privacy policy forms part of the overall agreement
Ovusense	Not medical advice	Not liable for any damages; Liability for defective goods cannot exceed the price of the product	Contract for sale and delivery of the wearable	English law; Non-exclusive jurisdiction	Not mentioned
TempDrop	Not medical advice	Not liable to the fullest extent permitted by law	Not liable under any contract	State of Israel	Privacy policy forms part of the overall agreement
WeVibe	No guarantee of quality, functionality, protection from computer viruses	Liable for foreseeable damages resulting from slight negligence; no limit to liability for gross negligence	Liable for breaches in contractual obligations (see box to the left)	Law of the Federal Republic of Germany, excluding the united Nations Convention on the International Sale of Goods.	Not mentioned
WHOOP	Not medical advice; Not a fitness instructor; AI generated information may be inaccurate. **Warranty: products will be free from defects for duration of user's subscription**	Liable for defective goods when warranty is effective - only liable for the cost of those goods	Contractually liable when warranty is effective	English law; Non-exclusive jurisdiction	Privacy policy forms part of the overall agreement

Disclaimers of Warranty

Most apps / wearables we surveyed included disclaimers of warranty. That is, they denied that the product / service they provided would meet certain specified standards of functionality. Many disclaimed a warranty regarding the accuracy of the information they provided as part of the service - e.g. "*You understand and agree that Natural Cycles in no way guarantees the accuracy of the Products' measurement outputs*."[131] Those that tracked fertility thus often made it clear that, given this lack of assured accuracy, they were not a substitute for contraception: "*THE APP IS NOT INTENDED TO…SERVE AS A BIRTH CONTROL METHOD OR CONTRACEPTION*". [132]

[131] Natural Cycles Terms of Use. Available at: natural cycles terms of use.
[132] Flo Terms of Use. Available at: https://www.owhealth.com/terms_of_use.html.

This disclaimer regarding accuracy was often coupled with a disclaimer declaring that the femtech product was not to be considered medical advice and was not a substitute for guidance from a medical professional. As Ovia Health stated: "*THIS IS FUNDAMENTALLY IMPORTANT: Ovia Health does not provide medical advice. Furthermore, the Services are not intended for use as a medical device and do not provide treatment or diagnoses*."[133] Similarly, as Elvie Trainer stated: "*There is no replacement for specialist medical advice from a qualified professional and we strongly recommend you seek such advice before using our products or services, or relying on the information provided via our platforms.*"[134]

14 apps and three wearables also issued disclaimers regarding the quality of third party content - e.g. Glow stated: "*you should be aware that all information included under the heading "Insight" is from the third party source listed with that information. While we believe the source of such information is reliable, we take no responsibility for its accuracy or applicability to your situation and you should review the underlying source (by clicking the hyperlink) before you make any material decisions based on it*."[135] This also applied to user-generated content visible to other users of the app.

Three apps and one wearable also included disclaimers about the use of their services by minors / those under a specified age. For example, Flo stated that "*The information within the app does not incite, induce or otherwise promote any sexual behavior or activity among minors and does not direct the content of communication to any particular person. All information provided within the app is for general educational purposes only*."[136]

Three apps and two wearables provided a disclaimer about algorithmic data processing. This was usually in the context of explaining that they could not guarantee the accuracy of results produced through this analysis:

> *"Lovense may provide AI-powered service or function ("AI service") by using technology provided by third-party service providers ("AI Provider")...Any use of the Output is at your sole risk, under the terms set forth herein and the terms of the specific AI Provider who provided the services with respect to an Output."*[137]

Most apps included 'as is' warranty disclaimers, and disclaimed 'to the extent permitted by law'. For example,

> "*The FEMM App and the content are provided on an "as is" basis. FEMM, its licensors, and its suppliers, to the fullest extent permitted by law, disclaim all warranties, either express or implied, statutory or otherwise, including but not limited*

[133] Ovia Privacy Policy. Available at: https://www.oviahealth.com/privacy-policy/.
[134] Elvie Terms of Use. Available at: https://www.elvie.com/en-gb/terms-and-conditions-of-use?srsltid=AfmBOooYcibi8GHmQTsl2tAozPD6ke3C2qGT5TyLnzJvg9dJ4L0k0UEV.
[135] Glow Terms of Service. Available at: https://glowing.com/terms-of-service?srsltid=AfmBOopo0OdVylAZa0we1znEMi-41chyA5ALFhfqBXXP_xNhBRvouh7d.
[136] Flo Terms of Use. Available at: https://www.owhealth.com/terms_of_use.html.
[137] Lovense Terms of Service, capitalisation in original. Available at: https://www.lovense.com/app/terms-conditions.

to the implied warranties of merchantability, non-infringement of third parties' rights, and fitness for particular purpose."[138]

These full disclaimers were sometimes accompanied by an exclusion clause noting that such comprehensive exclusion was not possible in certain jurisdictions: "*Exclusions: Some jurisdictions do not allow the exclusion of certain warranties or the exclusion or limitation of liability for consequential or incidental damages, so the limitations above may not apply to you."*[139]

Excluded Liability

Warranty disclaimers were usually accompanied by statements excluding the company from liability in regard to those warranties. That is, where they issued a warranty disclaimer indicating that the product / service would not meet certain standards, they also excluded liability on this basis. Thus, where they disclaimed any warranties regarding protecting user data from loss, they would also deny liability for this if the user's data was lost:

> "*You are solely responsible for the security of your personal user content. Except to the extent required by law, we accept no liability for the deletion, damage or failure to store user content maintained or transmitted through the use of the Clue Services."*[140]

As in the case of the disclaimers above, some denied liability for inaccurate information generated by the app based on a user's engagement with it:

> "*Without limiting the foregoing, FEMM, its licensors, and its suppliers make no representations or warranties about the following:*
>
> *The accuracy, reliability, completeness, currentness, or timeliness of the Content, software, text, graphics, links, or communications provided on or through the use of the FEMM App or FEMM."*[141]

Notably, such a statement did not appear in the Privacy Policy, indicating a significant difference between the two.

Eight apps and eight wearables excluded any liability. Flo is indicative:

> "*In no event shall the company or any of its officers, directors, agents, affiliates, employees, representatives, suppliers, partners, advertisers, or data providers be liable for any indirect, special, incidental, consequential, exemplary or punitive damages (including but not limited to loss of use, loss of profits, or loss of data) whether in an action in contract, tort (including but not limited to negligence), equity or otherwise, arising out of or in any way connected with the use or misuse of this app".*[142]

---

[138] FEMM Terms of Use. Available at: https://femmhealth.org/terms-of-use/.
[139] Frendo Terms of Use.
[140] Clue Terms of Service https://helloclue.com/terms.
[141] FEMM Terms of Use. Available at: https://femmhealth.org/terms-of-use/.
[142] Flo Terms of Use. Available at: https://www.owhealth.com/terms_of_use.html.

Other T&C accepted liability, but only for reasonably foreseeable damage.[143] They also accepted liability for damage to user's property (such as a user's phone) if this was caused by defective digital content and could not have been avoided by following the company's own advice. They noted that:

> "*However, we will not be liable for damage that you could have avoided by following our advice to apply an update offered to you free of charge or for damage that was caused by you failing to correctly follow installation instructions or to have in place the minimum system requirements advised by us."*[144]

Contractual Liability

Several apps and wearables specified that they would not be liable under any theory of law, or for breach of contract.[145]

Three apps and two wearables also incorporated a class action waiver, explicitly stating that users could only bring legal action against the given company as an individual and not as a member of a class (such as the class of 'user's of this app'). Spot On, for instance, stated that: "*You may not act as a class representative or private attorney general, nor participate as a member of a class of claimants, with respect to any Claim. Claims may not be arbitrated on a class or representative basis*."[146]

Ownership, licensing, and monetisation of data

Regarding ownership, licensing, and the monetisation of data, most made it clear that, by using the app, the user gave the company a worldwide, non-exclusive, sublicensable, assignable, royalty-free, perpetual, irrevocable right to use, host, store, reproduce, modify, create derivative works, and display and distribute any content a user uploads. Glow went even further, claiming they had an 'exclusive' licence to user's data.

Jurisdictions

Several apps / wearables provided a single jurisdiction for purposes of applicable law and/or forum, either a country or a state - e.g. Clover The Republic of Cyprus; FEMM the State of New York.[147] Stardust made it explicit that the laws of the State of New York would apply to users, regardless of their location:

> "*No matter where you're located, the laws of the state of New York will govern these Terms and the relationship between you and the Company as if you signed these Terms in New York…The parties agree to submit to the federal or state courts in New York for*

[143] Health and Her Menopause App. Available at: https://healthandher.com/pages/website-terms#:~:text=THE%20SERVICES%20PROVIDED%20ON%20OUR,COMPLETE%20INDIVIDUAL%20HEALTH%20SITUATION%20INTO.
[144] Ibid.
[145] Natural Cycles Terms of Use. Available at: natural cycles terms of use.
[146] Spot On Terms and Conditions. Available at: https://spoton.msu.edu/terms-conditions/.
[147] Clover Terms of Service. Available at: https://wachanga.com/eng/terms.

> ***exclusive*** *jurisdiction of any dispute arising out of or related to your use of the Services or your breach of these Terms*."[148]

Others mentioned multiple jurisdictions, depending on where a user was a resident. As Flo stated: "*If a resident of the US, then the relevant jurisdiction is either Delaware or the State where the complainant resides. If a resistant of EU, UK, Switzerland, Norway or Iceland: the courts of your usual place of residence*."[149]

Stardust, for example opted for English law as the applicable law, but gave "the courts of England and Wales' only 'non-exclusive jurisdiction".[150]

Notably, in this context, Clue stated that they would be entitled to sue the user on the basis of the laws in the user's own jurisdiction:

> "*Jurisdiction: To the extent permissible by law, all disputes arising under these Terms shall be heard in the courts of our registered place of business in Berlin, Germany. Notwithstanding the foregoing, we are also entitled to sue you under these Terms in your place of domicile*."[151]

Distinction Between Wearable and App / Hardware and Software

Of the wearables surveyed, several T & Cs made reference to this distinction, clarifying that the terms of service applied to that app, sometimes offering a separate terms of sale applying to the wearable device. Some offered terms that specifically applied to the wearable, e.g. a thirty-day money-back guarantee. Oura referenced the physical nature of the device, detailing the specific physical dangers it could pose to users:

> "*Please be cautious that the Product you are wearing does not get caught on fixed structures or heavy objects. If you experience redness or skin irritation on your finger while wearing the Product, remove it immediately. If symptoms persist longer than 2-3 days of not using the Product, please contact a medical professional. Our Product should not be placed in the mouth at any time. Oura's Product is not a toy nor is it intended for use by children. Children should not be left unattended with this Product, as it may pose a choking hazard*."[152]

Relationship Between The Terms of Service and The Privacy Policy

Most terms of service made reference to the privacy policy but often did not make it clear how the privacy policy was incorporated into the terms of service. Those that did, usually stated that the two should be taken together, both forming part of the overall agreement with the user.

---

[148] Stardust, Terms of Service (emphasis added). Available at: https://stardust.app/terms-of-use.html.
[149] Flo Terms of Use. Available at: https://www.owhealth.com/terms_of_use.html.
[150] Stardust Terms of Service 19.9. Available at: https://moodymonth.com/terms-of-use.
[151] Clue Terms of Service https://helloclue.com/terms.
[152] Oura Terms of Use. Available at: https://ouraring.com/terms-and-conditions?srsltid=AfmBOopH_IVZ8ZO_woHJGYDZgrYCMMGiM269Sn9lqZT_S0A1qRuRJugP.

Overall, some disclaimers included in the T & Cs were not mirrored in the privacy policies. Indeed, the privacy policies sometimes contained initial statements claiming that the user's privacy / data security was a top priority, while the terms of use were careful to disclaim any guarantee regarding complete data security. This, coupled with an absence of discussion of the company's lack of liability if a user were to lose data as a result of using the app, may create a misleading picture. A user may feel a false sense of security upon reading the privacy policy that is not supported by what is present in the terms of service / use. Many terms of service also did not explain how they related to the privacy policy, suggesting a lack of clear continuity between the two.

Conclusions

This study has provided an overview of current femtech data handling practices by undertaking an empirical analysis of the Privacy Policy and Terms and Conditions of 42 femtech apps including 15 wearables. The empirical analysis of these documents was combined with a legal assessment of their compliance with data protection law and in particular the GDPR. The report offers important and timely findings to support more informed debates in the area as well as to inform future research.

Three points stand out: First, the research showed that **femtech's questionable data processing compliance with the GDPR is of serious concern** because it might result in **data privacy gendered risks**.[153] This is particularly problematic because as some of us have argued elsewhere, the GPDR itself -despite being widely considered 'the gold standard' for data protection laws worldwide-[154] currently fails to explicitly recognise gender in the special categories of data under Article 9 GDPR, and, concomitantly, to adequately address gendered data risks and harms.[155]

Second, despite GDPR's commitment in theory that consent as a ground for lawful processing be informed and free, practices which are in fact treated as conforming with the informed consent standard, would be considered as unlawful under the equivalent informed consent standard applied in the medical context. As we explain elsewhere, since at least in the case of wearables, femtech apps make contact with the body for medical reasons (broadly defined), it makes sense that the (stricter) tests for securing informed consent in the medical context would apply to femtech wearables.[156]

Third, this study acknowledges that femtech is situated within a **broader social and medical context** characterised by substantial **knowledge gaps regarding women's sexual and reproductive health**; (dangerously) under-resourced and over-stretched public health services; uphill battles that women face when seeking diagnosis and treatment for gynaecological symptoms and conditions; and, a widely recognised tendency to question whether women are trustworthy narrators of their own health and pain, particularly regarding conditions related to the (dis)functioning of their reproductive organs.[157]

It is in the light of the above that the study draws a number of concluding remarks and recommendations. Crucially, despite the problematic compliance the present research revealed with regard to data processing by femtech actors, this report is cautious in its recommendations to femtech users as the burden should not be placed on them.

---

[153] Siapka, Tzanou and Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.

[154] See, inter alia, G Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016) 6 *International Data Privacy Law* 77.

[155] For a detailed analysis, see Siapka, Tzanou and Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.

[156] Tsachi Keren-Paz, Anna Nelson & Maria Tzanou, 'Femtech wearables and embodied harm: a new regulatory approach' (under review, 2025).

[157] Siapka, Tzanou and Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR', 112-113.

The study identified several elements of what can be characterised as **GDPR-compliant practice** in certain femtech Privacy Policies. These included: the offering of services without the need to collect personal data; the clear acknowledgment of the categories of data processed and their sensitivity and an established differentiation as to their processing; the recognition of appropriate and relevant legal bases for processing; the storage of femtech data locally on users' devices in a non-identifiable manner; a degree of appreciation of the potential risks and harms of sharing femtech data with law enforcement authorities, including a willingness to review such requests and to notify users before sharing any data or -for specific apps- to resist such requests altogether; an option allowing users to delete all their data when needed; the possibility to display a fake screen in case someone asked the user to open the app and they did not want them to see their data, for instance, in cases of (sexual and reproductive) intimate partner surveillance or surveillance by other family members.

However, of concern is that there were **discrepancies among apps** on the extent to which **they incorporated such practices** or indeed **discrepancies within the same app** (whereby they adhered to some of these practices but not others) resulting in partial compliance with GDPR obligations.

One of the ways in which some femtech apps market themselves is through their ability to contribute towards better understanding of women's health, which has thus far been under-researched.[158] This 'empowerment' rhetoric appears misleading as this study showed that the **consent** sought to use **users' data for research** is based on **vague statements** that **fail to provide data subjects with clear information** about the methods used to protect their data and about such research, including what it entails, who is involved in this, by whom it is funded, whether it is subject to ethics oversight, etc. The information given to users and the regulatory oversight of such research, at least that done in-house, **fall short** significantly from the practice in **clinical research settings**.[159]

Several practices identified in the Privacy Policies of the surveyed femtech apps and wearables raise reasons for **concern**. Such practices are not just 'unfair and unsafe'.[160] They are **unlawful** as they **fail to comply with the GDPR**. Divergences with regard to compliance were also observed within the same app's Privacy Policy. It was often the case that a certain app was found to comply with **some** (but not all) of their GDPR's requirements. **Partial compliance** is still **problematic** and **unlawful**. These divergences demonstrate that the overall picture of femtech's compliance with data protection law -even for Privacy Policies identified as good practice- is a **complex** and **nuanced** assessment followed by a number of caveats.

The study identified **several problematic aspects** regarding femtech apps' Privacy Policies and Terms and Conditions:

[158] Maya Dusenbery, *Doing Harm: The Truth about How Bad Medicine and Lazy Science Leave Women Dismissed, Misdiagnosed, and* Sick (HarperOne 2018); "Editorial: Funding research on women's health" (2024) 2 *Nature Rev Bioeng* 797–798 (2024). https://doi.org/10.1038/s44222-024-00253-7

[159] We plan to substantiate this point in a future academic output.

[160] Kemp, 'Your Body, Our Data: Unfair and Unsafe Privacy Practices of Popular Fertility Apps'.

- Femtech privacy policies were **ambiguous** and **lacked overall certainty**. Femtech data are particularly **intimate** as they concern **women's sexual and reproductive health**. Yet, we found that certain policies **failed** to recognise that these are data concerning **health** and/ or a natural person's sex life or sexual orientation. Some policies also failed to **clearly articulate** whether any heightened protections are provided to such data as required by the GDPR. Generic qualifications referring to 'wellness' or 'health' data without further clarifications about the protection offered to these as well as to data that could act as proxy to such sensitive and intimate information could raise confusion to users.

- Privacy policies **varied** as to **what extent** and **how** they demonstrated compliance with the GDPR's **data protection principles** of transparency of processing, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality. This makes the overall **fairness of processing** by femtech apps and wearables **dubious**.

- Of concern is that Privacy Policies sometimes failed to provide a **clear legal basis** for processing or mentioned multiple legal bases under the GDPR or other purposes without any further clarification. This can be very **confusing** and raises concerns about the **lawfulness of processing**.

- We have serious concerns about the use of **consent** as a legal basis in the femtech context. These regard, first, the **non or partial compliance** of femtech apps and wearables with the GDPR's requirements of consent for the processing of **special categories of data**. Besides the fact that some of current practices by controllers should be considered as non-compliant according to GDPR's existing consent requirement (which is misapplied), secondly, **the GDPR's current consent test**, even when applied correctly, **falls short** from what is needed to **adequately guarantee users' autonomy**.[161] For example, non-compliance about the way the information is processed might be—and has been[162]—considered as 'mere loss of control', namely one that does not cause any 'real' loss, not even discernible distress, and therefore does not justify (according to the ICO) a regulatory action by the ICO; nor the award of damages (according to *Lloyd v Google*[163]).

- The report found **no notable differences** in Privacy Policies **between apps** and **wearables** regarding the protections afforded. We find this surprising as wearables might produce **further harms** to the potential data harms that might arise from apps; these **harms are embodied** in the narrow sense—they have to do with the undermining of bodily integrity due to the fact that an intimate wearable is worn without adequately

[161] Keren-Paz, Nelson & Tzanou, 'Femtech wearables and embodied harm: a new regulatory approach'. In both medical and sexual contexts only mistake about the **nature** of the interaction vitiates consent. Mistake about the **circumstances**, including about the relevant **risks**, only allows for a claim in negligence and is **limited to physical**, to the exclusion of purely dignitary, harm.
[162] ICO, 'PACE Project: Fertility & Menstruation Apps – Internal Report' (2024) redacted version.
[163] [2021] UKSC 50.

informed consent. These **additional** harms should not be ignored in the femtech context, where wearables and sextech are worn on **women's reproductive organs**, thus raising concerns of undermining users' **bodily integrity.** These harms are enhanced by but are also independent of informational/ data related harms.[164]

- Privacy Policies which stated that "We **may** share your data" with third parties **without clarifying the identity of these third parties** and in which cases data is shared are unacceptably **vague**. Ambiguous language ("may") contributes to lack of clarity, and risks **undermining informed consent** in cases of **femtech data sharing** as the question of whether or not data will be shared is a material one.

- Sharing data for **personalised ads** seems to be a **common practice** in the surveyed apps. The research has found that femtech apps and third parties, such as Google and Facebook may **observe users' activities, preferences, and transactional data** (such as IP address and browser type) as well as **content they have viewed** during their use of the service. This is **sometimes (but not always)** acknowledged in Privacy Policies, albeit in an obscure and **misleading way** which raises doubts about the **lawfulness** and **transparency of processing** as well as the level of agency or choice of the users. We observe that although third-party sharing is often considered essential to the business models of several digital technologies, when performed in the femtech context, it **predominantly** relies on and **affects women**.[165] Such marketing practices for which this data sharing is employed are **gendered**, capitalising on data related to reproductive milestones and enabling the segmentation of marketing targets into reproduction-related profiles. These assumptions could **produce gendered data harms**[166] as they feed into advertising practices which, unbeknownst to the femtech users on whose data they rely, might be experienced by women as **unnecessary** and **creepy** or even **shameful** and **upsetting**, depending on their individual circumstances (for example, being targeted with Facebook ads about baby products when a woman has suffered a stillbirth).[167]

- **Sharing data** with third parties for **research purposes** seems to be a **common practice** in the surveyed apps. This is usually not done with sufficient level of transparency and detail. Only one Privacy Policy mentioned that the company may receive compensation for sharing de-identified or aggregate users' data, only a handful of Privacy policies clarified that separate, special consent will be required. The policies did not mention (a) the identity of the research partners; (b) their status as private, public non/academic institutions; (c) their sources of funding and (d) what type (if any) of regulatory oversight they are subject to. Finally, there is no clear distinction between in-house

[164] Keren-Paz, Nelson and Tzanou, 'Femtech wearables and embodied harm: a new regulatory approach'.
[165] Siapka, Tzanou, Nelson 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.
[166] For a definition, see ibid.
[167] Gillian Brockwell, 'Dear tech companies, I don't want to see pregnancy ads after my child was stillborn' *The Washington Post* (Washington DC, 12 Dec 2018). Available at: www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/.

processing for research & development purposes and research involving sharing of the data with third parties; the status of the former as akin to or as distinct from 'clinical research' and they way, if at all, it is subject to any ethical oversight was not mentioned at all.

- **AI** is used in the femtech industry which promises to make **algorithmic predictions** on future periods, pregnancy and other gynaecological conditions. It is, therefore, surprising that the study of Privacy Policies found **minimal references** to AI and in particular to the **conditions under which this is employed**. Even more worrying is that the research found **no mentions of specific guarantees** applicable when AI is used to analyse women's sexual and reproductive data and generate relevant predictions.

- Femtech apps might help **teenage girls** to understand their changing bodies and their menstrual and sexual health. However, it is concerning that relevant Privacy Policies only mentioned different **age requirements** for processing children's data, but did not provide any details on potential **heightened protections** for processing of such data in this context. The processing of girls'/ children's -considered vulnerable data subjects under the GDPR- intimate data should be taken **seriously** as it could lead to **individual** and **collective gendered data harms**, including increased surveillance of girls' bodies and reproductive autonomy by parents, family members, partners, private actors or public authorities.

- There were **considerable differences** between the surveyed Policies as to which **data subjects rights** -right of access, right to rectification, right to restriction of processing, right to data portability and right to object- were guaranteed to users and how the latter could **exercise** them. Some Privacy Policies merely listed the data protection rights without providing any further explanation as to how these could be exercised by the data subject. This is problematic and indeed non-compliant with the GDPR to the extent that it makes it very difficult (excessively time consuming, costly) or impossible to data subjects' to exercise their rights.

- The report revealed **concerning discrepancies** between **Privacy Policies** and **Terms of Service**. Statements made in Privacy Policies, in particular regarding **data security** and the **accuracy** of femtech apps' predictions were often **explicitly disclaimed** in the Terms of Service. This is worrying because it can create significant confusion to users. For users reading only the Privacy Policies this is outright **misleading** as they might have **relied** on these statements in deciding to use the app. It also shows that femtech users are ultimately not given any **real agency** when agreeing to Privacy Policies and Terms of Service if the two are **contradictory**. We also found it troubling that Terms of Service sometimes **shifted the burden of responsibility to data subjects**, essentially asking them to fend **for their own data security**.

- Provisions regarding the duration of **data retention** in the surveyed Privacy Policies were often **confusing** and **misleading** as they failed altogether to provide any retention

time periods; mentioned duration of retention that was not sufficiently clear to users; provided unnecessarily excessive retention time periods; failed to give an indication of whether the data would be deleted once these expired; and continued to maintain the data even after the users had deactivated their account.

- The overwhelming majority of surveyed policies did **not mention** anything about **data protection impact assessments (DPIAs)**. This is **regrettable** given the **sensitivity** of femtech data and the potential **seriousness** of relevant (gendered) **data risks and harms**. DPIAs and in particular **femtech sector DPIAs** which **involve users' input** could play an important **role** in **addressing collectively** the areas of concern identified in this report.

Recommendations

Femtech companies:

1. Femtech privacy policies should be written in a **clear** and **transparent** way which **complies with the GDPR**.

2. The **different categories of data** processed in the femtech context, their **intimate** and **gendered** nature should be recognised and **enhanced protections** should be provided for data concerning health or a natural person's sex life or sexual orientation.

3. It should be acknowledged that in the femtech context even **non-sensitive data**, such as device information or patterns of app use could act as **proxies to intimate information** about women and their bodies. Such data should be protected accordingly.

4. **Substantive compliance** of privacy policies with the GDPR should be ensured, in particular with the **data protection principles** therein: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and, accountability. Partial compliance with some but not all the obligations under the GDPR is not sufficient and raises questions about the **fairness** and ultimately the **lawfulness of processing**. Partial/ non-compliance could make controllers subject to investigations by supervisory authorities, fines and judicial proceedings.

5. The **relevant, appropriate legal basis** for processing personal data in this context should be identified. More than one legal basis can be used but it should be clearly explained to users why a specific legal basis is employed for a specific purpose and how it corresponds to the processing of relevant data.

6. When **consent** is used as a legal basis, it should be ensured that privacy policies enable **explicit, freely given, specific, informed** and **unambiguous** indication of the data subject's wishes by which she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to her.

7. **Ambiguous, confusing and misleading wording** regarding femtech data processing and sharing with third parties should be **avoided** as it undermines the very essence of informed consent.

8. **Sharing data** with third parties for personalised ads should be **properly acknowledged** in the Privacy Policy which should clearly list **all the relevant third parties** with whom the data is shared. Users should be allowed to opt out from such a practice without losing access to the app or its functionality.

9. **Sharing data** with third parties for **research purposes** should be **properly acknowledged** in the Privacy Policy which should clearly list **all the relevant third parties** with whom the data is shared, **their status**, **their sources of funding**, **and whether the controller is paid for**

the data shared. **Specific** consent for this purpose should be secured and users should be allowed to opt out from such a practice. Users should also be notified whether their **data is used in-house in order to improve the algorithm's functionality**, including predictions' accuracy. The Policy should explain the nature of such 'research and development' use and how it is different from clinical research (or from research involving third parties which does not amount to clinical research). In particular, how (if at all) the research (whether in-house or not) is subject to regulatory or ethical oversight should be clarified.

10. The **use of algorithmic analytics, AI and chatbots** should be properly acknowledged if these are employed by a femtech app or wearable. The risks of such systems on women and girls and their reproductive and sexual health and autonomy should be properly assessed and the specific guarantees applicable in these cases should be clearly communicated to users.

11. Femtech apps which **process girls'/ children's data** should assess the potential relevant **gendered risks** and provide for **enhanced protections** for those **vulnerable data subjects**.

12. Privacy Policies of apps associated with **wearables** should acknowledge that the use of wearables implicates **bodily integrity** and not merely informational privacy. Compliance, and transparency about how the data is to be used are especially important in cases of intimate wearables given the additional protected value of **bodily autonomy** and integrity, and, in the context of sextech, **sexual autonomy**.

13. The **duration of time** in which different types of femtech data are to be retained should be clearly provided. This duration should comply with the **principle of proportionality**. Data should be **deleted** automatically once retention periods have expired (the possibility of a user re-activating their account should be taken into consideration).

14. Femtech policies should guarantee **all data subject rights** under the GDPR and should provide clear guidance to data subjects on **how to exercise them**. The exercise of such rights should be straightforward; it should not be costly, confusing, time demanding or rendered effectively impossible.

15. The protection of femtech generated data against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures is **of paramount importance** given the level of intimacy and sensitivity of such information. The **controllers** are **responsible for ensuring data security**. Such burden should not be shifted to data subjects.

16. A **Data Protection Officer (DPO)** should be in place and information about the DPO and their contact details should be clearly stated in the Privacy Policy of the app or the wearable. DPOs **monitor** data controllers' compliance with the GDPR and could, therefore, provide important guidance towards compliance.

17. **Data protection impact assessments (DPIAs)** covering all processing operations should be carried out. This could be undertaken **for a specific app/ wearable** or **collectively**. Data

controllers could perform collective 'femtech DPIAs' or 'Gender-focused DPIAs' or indeed 'feminist DPIAs'. The development of such sector-, technology- or target group-specific DPIA frameworks is better suited to account for the more **collective** sorts of risks of femtech and its consequences on particular groups. A **femtech sector-specific approach to DPIA** frameworks would be able to draw on the accumulated sectoral knowledge and address risks arising from relevant data processing activities in a targeted and detailed manner.[168] Such collective femtech DPIAs should consider not only high-risk data processing but also broader risky outcomes (i.e., potential violations of rights, including sexual and reproductive rights). It is crucial that **data subjects' engagement** is sought by controllers when developing 'femtech DPIAs'. Given that risks are varied and often subjective, their assessment would benefit from becoming more **participative**.[169] **Public involvement** of femtech users (or women more broadly) could help achieve a more comprehensive framing of the relevant risks, factoring in data subjects' knowledge and context, particularly with respect to **gendered risks**- be they individual, embodied, collective or societal.[170]

Users:

Femtech might be a helpful tool for users seeking to track and manage their sexual and reproductive health given the significant limitations and underfunding of women's health services. This report is cautious **not to place the onus of ensuring that users' privacy and data subject rights are adequately protected on femtech users**.

Accountability for complying with legal obligations falls on **controllers** and the **monitoring** and **effective enforcement of compliance** with the GDPR should be undertaken by **Data Protection Authorities** (**DPAs)**.

Compliance with data protection requirements is a **legal obligation** for femtech companies. Users should not feel powerless if Privacy Policies are unclear, confusing or misleading. There are a number of legal mechanisms and rights at place available to users to ensure enforcement of the law.

1. At the **individual level,** at first instance, femtech users could exercise their **data access right** (and other data subject rights) against controllers. Data access could help users identify **what data** a femtech app or wearable has collected about them, **how** and **why** such data **is processed**, **with whom** it is shared, and for what purposes. More broadly, it could give users an indication

[168] This is recommended by the WP29 itself, which suggests that 'a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing'. More concretely, this applies to cases of (i) data processing within a particular sector; (ii) use of similar technologies for data processing; or (iii) similar data processing activities. This suggestion is made in Siapka, Tzanou, Nelson 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.

[169] This is facilitated by Article 35(9) of the GDPR 'Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations).

[170] See Siapka, Tzanou, Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.

about the **lawfulness** of the data processing and it could be important to **exercise other data subject rights** or **file a complaint** with a DPA.

2. Users who have suffered data harms (or more broadly loss of privacy) as a result of femtech's practices which fail to comply with the GDPR could **lodge a complaint** with a supervisory authority/ **DPA** in the Member State of their habitual residence, place of work or place of the alleged infringement.[171] This is a fairly simple and inexpensive way to pursue potential complaints. If users are not satisfied with the outcome of the DPA's investigation of their complaint, users have the right to judicially challenge a legally binding decision of a DPA concerning them before the **courts**.[172] Users can also bring a court case if the DPA has not informed them about the progress of their complaint within three months.[173]

3. Users could also bring **judicial proceedings** directly against a femtech controller (or processor) where they consider that their rights under the GDPR have been infringed as a result of non-compliant processing of their personal data.[174] Users can also consider a civil claim against the controller in tort law (misuse of private information, and in cases of wearables, also potentially negligence and battery).[175] This report recognises, however, that it might prohibitively expensive and extremely time-consuming to engage in court's action at the individual level.

While **individual data harms** occur in the context of femtech and pursuing individual complaints is an important avenue, data harms that users suffer as an individual might be identical/ similar to harms suffered by other femtech users. **Collaboration** and **collective action** might give femtech users more chances to succeed in their complaints. Crucially, even if femtech's data privacy policies appear compliant with the GDPR or users feel that they have not personally suffered any negative impact, it might still be that the femtech gendered processing of intimate data might lead to **broader societal injustices** or have a **discriminatory**, **exclusionary** or **unfair effect on women's sexual and reproductive autonomy in general.**

4. Femtech users could resort to **collective means of action** to deal with **individual, collective** and **societal harms**. Such collective action can be understood as procedural **class action** and/or positive protection to advance a collective interest. The GDPR is more oriented in protecting individual rights and therefore it might be challenging to incorporate collective or societal gendered harm in its approach. However, the 'strength in numbers' of femtech users could help challenge the gendered risks of large-scale data-driven technologies, such as femtech.[176] This

[171] Art. 77 GDPR.
[172] Art. 78 (1) GDPR.
[173] Art. 78 (2) GDPR.
[174] Art. 79 GDPR. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has her habitual residence.
[175] Keren-Paz, Nelson and Tzanou, 'Femtech wearables and embodied harm: a new regulatory approach'.
[176] Jef Ausloos, Jill Toh and Alexandra Giannopoulou, 'The Case for Collective Action against the Harms of Data-Driven Technologies' (*Ada Lovelace Institute*, 23 November 2022). Available at: www.adalovelaceinstitute.org/blog/collective-action-harms/.

means that data rights under the GDPR could help bring together **groups** of women **who share related issues** and 'place **agency** in their hands **to build momentum for broad sets of collective goals'**[177] in the femtech context. We note, however, that in the UK, the effectiveness and viability of representative action for data harm was significantly reduced in the Supreme Court decision of *Lloyd v Google.*[178]

Article 80 of the GDPR allows **not-for-profit bodies, organisations or associations** (e.g., civil society organisations, digital rights non-profits, consumer associations, trade unions) **to start an action on behalf of data subjects** (with or without the latter's mandate) albeit under certain conditions and differing national transpositions.[179] This is important because users might not necessarily have the (informational or financial) capacity to exercise their rights against resourceful data controllers on an individual basis but may instead require **coordination on a collective level**.[180] To that end, (collectively) exercising the right of access -mentioned above- could serve as a **means to identify the violation(s) on which subsequent femtech litigation can be based** and to potentially help femtech users discern the collective rather than individual risks to which they are exposed. [181]

Data Protection Authorities (DPAs):

1. DPAs should **(pro)-actively monitor compliance** of femtech apps and wearables with the GDPR. They should ensure proper enforcement of the GDPR in this context.

The review of period and fertility tracking apps by the UK's Information Commissioner's Office (ICO)[182] was a promising example of such an assessment. However, it is **disappointing** that the ICO's full report[183] contains contradictory conclusions. For instance, the ICO noted that: 'initial findings' point to 'excessive data collection, inappropriate lawful bases being relied upon/failure to obtain valid consent, a general lack of transparency, inadequate security measures and an overall lack of accountability'.[184] Nevertheless, the ICO's conclusion was that '[w]e do not have evidence that period and fertility apps named in this report are misusing users' sensitive personal data relating to menstruation and fertility in a way which causes harm. We do not have evidence that the apps are sharing special category data for unjustified purposes, nor sharing special category data for the purposes of advertising. Where special

[177] Ibid.
[178] [2021] UKSC 50.
[179] Maria Tzanou and Plixavra Vogiatzoglou, 'Mapping Data Protection Legal Mobilization before the CJEU: The Need to Rethink a Success Story?' Nordic Journal of European Law (2024), 96;
[180] Jef Ausloos, Jill Toh and Alexandra Giannopoulou; Siapka, Tzanou, Nelson 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.
[181] René LP Mahieu and Jef Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (*Internet Policy Review*, 6 July 2020). Available at: www.policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487; Ausloos, Toh and Giannopoulou (n 212).
[182] ICO, 'PACE Project: Fertility & Menstruation Apps – Internal Report' (2024) redacted version.
[183] ibid.
[184] Ibid.

category data is shared for other purposes, the relevant apps correctly rely on explicit consent.'[185]

2. DPAs should **effectively handle complaints by femtech users/ data subjects** and **civil society organizations**.[186] This is important because it could initiate further debates and broader awareness in the area. It is also significant as evidence shows that such complaints under the GDPR seem to be limited at the moment.[187]

3. DPAs **should not shift the burden on data subjects**/ femtech users. The ICO's report is concerning in this regard. The report noted that 'users, may be inadvertently losing control of their data because they are not able to make, or aware they have the right to make, granular choices about what processing or sharing they are or aren't willing to consent to. However, this potential "loss of control" does not appear to be leading to any specific harms.'[188] We strongly disagree with this observation; as this report has shown **there are specific harms** arising in the femtech context and in particular **gendered data harms**. We would like to see DPAs **recognising these harms properly** and **actively enforcing the GDPR** when it comes to women's and girls' sexual and reproductive rights and autonomy.

4. Considerations of gendered risks could be made prominent in relevant DPA interpretations and guidance. The GDPR suggests the provision of guidance by codes of conduct, certifications, EDPB guidelines and data protection officers, **all of which could ensure the inclusion of gendered risks**.[189] In that regard, **the role of DPAs is pivotal**. DPAs could specifically **direct controllers' attention to gendered risks**, **raise awareness** about these and **ensure that data subjects have access to redress mechanisms** where such risks materialise.[190]

Policy-makers:

1. The GDPR should **explicitly recognise gender** and the possibility of **gendered risks**. This could be done by including gender as one of the 'special categories' of processing.

Article 9 GDPR currently establishes an in principle prohibition of processing of sensitive data because there is a risk that this might lead to, *among others*, discrimination, on the basis of

[185] We contrast the ICO's findings with ours in Keren-Paz, Nelson and Tzanou 'Femtech wearables and embodied harm: a new regulatory approach'.
[186] Art. 57(f) GDPR.
[187] For instance, the ICO PACE Report mentioned that the ICO had only received one complaint relating to operability. See also, Keren-Paz, Nelson and Tzanou, 'Femtech wearables and embodied harm: a new regulatory approach'.
[188] The ICO's report also notes before the above statement that 'users confess to not engaging with the privacy notices of the fertility and menstruation apps they use. While this does not absolve app developers of their data protection and accountability obligations, a lack of user engagement has arguably allowed such practices to proliferate and go unchecked. This is likely to be symptomatic of app usage more generally and not specific to fertility and menstruation apps. We found there to be a lack of transparency or insufficient information on data processing and, consequently, a reliance on bundled consent declarations.'
[189] Recital 77 GDPR.
[190] Siapka, Tzanou, Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.

personal data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. It, however, **does not mention 'gender' or 'sex'**. This is a **significant oversight** of the EU legislator in light of **Article 21(1) of the EU Charter of Fundamental Rights** (EUCFR), which provides that 'any discrimination based on any ground such as ***sex,*** race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited'.[191]

The GDPR's gender blindness **is not innocuous**; it reveals **a lack of acknowledgment of the significance of data protection rights for the safeguarding of women's sexual and reproductive health and autonomy**. As this study demonstrated, technology-facilitated gendered surveillance and gendered outcomes are inextricably linked with the sexual and reproductive rights of women and girls (or the lack thereof). **Personal data** (and data gaps), **data subjects**[192] and **risks of processing** can be **gendered**.[193]

Admittedly, sexual and reproductive data is 'data concerning health'[194] and, thus, falls within the special categories of data under the GDPR. However, this is **not sufficient**; the law should **explicitly acknowledge** that such data and more importantly their processing might entail **gendered risks associated with sexual and reproductive autonomy**, which are intrinsic to every woman and girl. An explicit mention of gender in the GDPR would significantly **strengthen the protection of women's sexual and reproductive rights** including in the femtech context. The **European Commission** and the UK legislator should seriously consider this urgently needed amendment to the GDPR.

2. Local, national and EU policymakers should **meaningfully engage women (and others who use femtech apps such as non-binary and trans people)** in law making initiatives and or amendments of existing legislation. They should include (representatives of) women's groups that are **subject to collective gendered risks** -including in the context of femtech- across all stages of 'law-making, policy, agenda and strategy setting, litigation, advocacy' as well as 'throughout standardisation processes and broader discussions of technology and digital rights'.[195]

3. Given the prominent health aspect of femtech, regulatory oversight from policy makers and regulators focusing on health is desirable. In particular, input from reproductive heath and gender equality in health care such as the Women's Health Ambassador, the Medicines and

[191] Emphasis added.

[192] Gianclaudio Malgieri and Gloria Gonz á lez Fuster , 'The Vulnerable Data Subject: A Gendered Data Subject?' (2022) 13 *European Journal of Law and Technology* 1, 1 .

[193] Siapka, Tzanou, Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.

[194] These are defined in GDPR art 4(15) as 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'.

[195] Jef Ausloos, Jill Toh and Alexandra Giannopoulou, 'The Role of Collective Action in Ensuring Data Justice' (*Ada Lovelace Institute*, 1 December 2022). Available at: www.adalovelaceinstitute.org/blog/data-collective-action-justice/.

Healthcare products Regulatory Agency (MHRA) and possibly, the Human Fertilisation & Embryology Authority.[196] Our report acknowledges, however, that the near ubiquitous disclaimer that femtech apps are not a medical device makes health-focused regulatory input unlikely.[197]

4. Given the prominent gendered nature of femtech and its harms, and the limited incorporation of gender justice into the current data protection regulatory space, regulatory oversight from policy makers, regulators and academics who focus on **gender equality** is desirable. Examples include the Women and Equalities Unit, the Gender Equality and Policy Hub and the Equality and Human Rights Commission (in the UK).

Courts:

1. **National** and **EU courts** have an important role to play in r**ecognising gendered risks within EU data protection law**.[198] In particular, the Court of Justice of the European Union (CJEU's) widely celebrated pro-data protection/ fundamental rights approach could further develop to **explicitly acknowledge gendered concerns** and **their link with women's and girls' sexual and reproductive rights**.[199]

2. At least in the case of **wearables**, but possibly **beyond**, the test for informed consent regarding the use of the data and (if applicable) the wearing of the wearable should be recognised to equate with the test used in the medical context.[200]

3. For **wearables**, both **informational** and **physical** harms ensuing from wearing a wearable and the gathering of personal data that would not have occurred had the user been informed **should be remedied** by courts**.** Possible causes of action include **data protection**, **misuse of private information**, **negligence** and **battery**. Misuse of private information is probably the tort most capable -in English law- of remedying both types of harm.[201]

---

[196] While the *Women's Health Strategy for England* (DHSC, 2022) https://www.gov.uk/government/publications/womens-health-strategy-for-england/womens-health-strategy-for-england#implementation-and-monitoring-progress refers to femtech in the report, its outlook is mainly positive, disregarding the risks discussed in our report. For example, in the digital heath technologies section (part of '10 Digital and Data'), immediately after a paragraph defining femtech, the report proceeds: 'We want to see greater use of digital technologies to empower women by demystifying and simplifying the process for companies to scale and launch their products in the UK'.

[197] For health care providers responsibilities with regards to recommending the use of Femtech see Anna Nelson, Maria Tzanou and Tsachi Keren-Paz, 'Recommending Privately-Developed FemTech in Healthcare Part 1: Promises and Pitfalls', *BMJ Sexual and Reproductive Health Blog*, September 16 2024 (here) and 'Part 2: 'Understanding Healthcare Professionals' Responsibilities' *BMJ Sexual and Reproductive Health Blog*, October 3 2024 (here).

[198] Siapka, Tzanou, Nelson, 'Re-imagining Data Protection: Femtech and Gendered Risks in the GDPR'.

[199] Ibid.

[200] Keren-Paz, Nelson & Tzanou 'Femtech wearables and embodied harm: a new regulatory approach'

[201] Ibid.

4. **English courts** should interpret the Data Protection Act 2018 as allowing the award of damages for mere loss of control.[202] More broadly, the restrictive English approach to data class actions should be reconsidered. **Courts** across **EU Member States** should also be receptive of collective actions within the GDPR and beyond.

Civil society, media and academia:

Femtech should be understood as a site in which **informational privacy** and **data protection intersects** with **reproductive** and **sexual health**, **gender equality** and (at least with respect to wearables) **bodily integrity** and **physical privacy**. Accordingly, civil society organisations from all relevant areas and academics from all relevant disciplines should engage with this area. It should be recognised that this is an inherent issue which should concern all those working in cognisant disciplines, and not a matter which can be left merely to feminist activists and scholars. Alongside the empowering potential of femtech—which, as we have seen, is highlighted in both industry and policy talk—the **harms** and **risks** from femtech should be **monitored**, **mitigated** and **remedied**. The media, which already highlights such risks,[203] should continue to do so.

[202] The GDPR remedies mere loss of control, but a UK Supreme Court decision ruled this out. See Keren-Paz, Nelson and Tzanou, 'Femtech wearables and embodied harm: a new regulatory approach'.

[203] For a recent coverage of among other functionality concerns see Alexandra Topping, 'UK women share their experiences of using fertility-tracking apps', *The Guardian* 14.01.2025 https://www.theguardian.com/society/2025/jan/14/uk-women-share-experiences-fertility-tracking-apps-contraception-pill-pregnancy#:~:text="I've%20tracked%20my%20periods,pregnant%20with%20our%20first%20child.
In the United States, following the abolition of a constitutional Federal right to abortion in Dobbs, media coverage dealt also with risk posed by period tracking apps. See Geoffrey A. Fowler and Tatum Hunter, For people seeking abortions, digital privacy is suddenly critical (Washington Post, 24 June 2022) https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/.