

# Privacy Notice for Study Participants

<b>Audience</b>	Adult study participants
<b>Document status</b>	Version 1.0; prepared for DST legal / ethics / insurance review

This Privacy Notice explains how personal data are collected, used, stored, shared, and protected in connection with DST's research and development activities. Please read it together with the applicable Participant Information Sheet and the Equipment Loan, Safe Use and Return Terms.

## 1. Who is responsible for your personal data?

The table below should identify every controller or joint controller that decides why and how your personal data are processed for this study.

Organisation	Role	Contact details
Deep Sleep Technologies B.V.	Controller or joint controller	Weesperplein 4B, 1018 XA Amsterdam, The Netherlands; study team: deelname-onderzoek@fordeepsleep.com; privacy contact: privacy@fordeepsleep.com

## 2. Which personal data do we use?

Depending on the study set-up and your role in the study, DST may process some or all of the following categories of personal data:

- Identity and contact details, such as your name, email address, telephone number, postal address, participant ID, age or date of birth, and preferred contact details.
- Screening and eligibility information, including information relevant to whether the study is suitable and safe for you.
- Study data from questionnaires, app entries, and communications with the study team.
- Sensor and device data, which may include physiology (electroencephalography, electrooculography, electromyography, electrocardiography, photoplethysmography, accelerometry, respiration, functional near-infrared spectroscopy, magnetic resonance imaging, saliva samples, or similar), acoustic or event logs, device status, timestamps, and data quality indicators.
- Support, incident, troubleshooting, and complaint records.
- Shipping, handover, return, and equipment-log data, including device serial numbers linked to your participant ID.
- Compensation, payment, tax, and accounting data needed to pay you and meet legal obligations.

Some of these data - especially sleep, health-related questionnaire data, and certain sensor data - may qualify as special-category personal data under the GDPR.

## 3. Why do we use your data, and on what basis?

Your informed consent to participate in the study is not necessarily the same as the GDPR legal basis used for every processing activity. The table below shows the legal basis actually relied on for each purpose.

Purpose	Examples of data used	GDPR legal basis to confirm
Screening, enrolment, scheduling, shipping, onboarding, and participant support	Identity, contact details, eligibility information, equipment-logistics data	Explicit consent

Purpose	Examples of data used	GDPR legal basis to confirm
Running the study and collecting study measurements	Questionnaires, sensor data, timestamps, device data, participant ID	Explicit consent
Monitoring safety, troubleshooting, and handling incidents	Support records, incident logs, health-related reports, device status	Explicit consent
Data analysis, reports, scientific outputs, and audit trail	Coded study data, protocol records, quality-control records	Explicit consent
Compensation, tax, and accounting compliance	Name, address, date of birth, bank details, payment amounts, tax or reporting data	Legal obligation
Future research purposes	Coded data	Explicit consent

Processing of special-category personal data (including but not limited to health-related information) relies on explicit consent.

#### 4. Where do the data come from?

- Directly from you when you complete forms, questionnaires, screening steps, or communicate with the study team.
- From the study equipment and study software while you take part in the study.
- From shipping, return, payment, or support providers acting on DST's instructions.

#### 5. Who receives your data?

DST limits access to people and organisations that need the data for the study or for legal compliance.

- Authorised study staff and internal personnel at DST who need access for recruitment, support, data quality, safety, payments, or legal compliance.
- Service providers acting on DST's instructions, such as cloud-hosting providers, device-management providers, analytics providers, shipping partners, and payment or accounting providers.
- Professional advisers, auditors, insurers, regulators, ethics committees, or authorities where this is necessary or required by law.
- Other researchers, collaborators, and/or commercial partners where this is allowed by the study governance, consenting procedure, and/or the data-sharing arrangements in place.

If data shared with another party remain personal data, DST uses a contract or controlled-access arrangement that limits the recipient's use of the data. Unrestricted public release only uses data that are genuinely anonymised or sufficiently aggregated so that individuals are not reasonably identifiable.

#### 6. Are data transferred outside the EEA?

Some service providers may process personal data outside the European Economic Area (EEA). If that happens, DST should only transfer data where an adequacy decision applies or where appropriate safeguards - such as Standard Contractual Clauses - are in place.

If you want more information about the applicable safeguard for a particular transfer, you can ask the privacy contact listed in this notice.

## 7. How long do we keep your data?

Data category	Recommended structure for the final retention rule
Direct identifiers used for recruitment, scheduling, shipping, and participant support	As soon as possible, but at the latest within 1 year after your participation in this study.
Payment, tax, and accounting records	7 years after the end of the relevant financial year, or longer if required by law.
Anonymised data	May be kept without time limit because they are no longer personal data.

## 8. How do we protect your data?

- Use of participant IDs and coded datasets wherever reasonably possible.
- Role-based access controls so that only authorised people can see identifiable data.
- Encryption, secure storage, and vendor contracts with confidentiality and security obligations.
- Separate handling of direct identifiers and other data where possible.
- Audit trails, device-management controls, and remote-lock or remote-wipe measures where technically available.

DST carries out and documents any required data-protection impact assessment and vendor due-diligence before when applicable according to GDPR.

## 9. Your rights

Under the GDPR, you may have rights that include access, rectification, erasure, restriction, data portability where applicable, objection, and the right to complain to a supervisory authority.

Some rights can be limited where data must be kept to comply with law, preserve research integrity, protect safety follow-up, or establish, exercise, or defend legal claims. Withdrawal of consent does not affect processing that was already carried out lawfully before withdrawal.

## 10. How can you contact us or complain?

Topic	Contact
Study team	participate@fordeepsleep.com
Privacy contact	privacy@fordeepsleep.com
Supervisory authority	You may lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) or your local supervisory authority.

DST should respond within the applicable GDPR timelines.