

Privacy Policy

1	Policy statement	3
2	Accountability	3
3	What does the Company use your personal data for?	3
4	What personal data does the Company collect?	3
4.1	Employees and Contractors.....	3
4.2	Securitisation Repository system users	3
4.3	Outsourcing Contacts and Suppliers	3
5	How confidential is your data?	4
6	How secure is your data?.....	4
7	How long is personal data kept for?	4
8	Recording Company meetings	4
9	Rights in relation to the personal information held by the Company	4
9.1	Subject Access Request	4
9.2	Right to Rectification	4
9.3	Right to Erasure	4
9.4	Right to Restriction of Processing	5
9.5	Right to Data Portability	5
9.6	Right to Object.....	5
10	Accuracy of Personal Information	5
11	Data security breaches	5
12	Special Categories of Personal Data	5
13	Who to contact about your Personal Data	5
14	Complaint to Supervisory Authority	6
15	Changes to this Policy.....	6

1 **Policy statement**

SecRep B.V. (the “**Company**”) is committed to protecting the privacy, security and integrity of the personal data it holds about its staff, suppliers and customers. The Company will comply with the requirements of the UK Data Protection Act 2018 and the General Data Protection Regulation (“**GDPR**”) and take appropriate safety measures to protect all personal data. This Policy is published on the Company’s website.

We may amend this Privacy Policy from time to time, to comply with applicable laws and regulations or to meet our changing business requirements. You are encouraged to periodically review this page for the latest information on our privacy practices and amendments to this Privacy Policy. By continuing to use our platform, you agree to be bound by all updates and amendments.

2 **Accountability**

The Risk and Compliance Officer (the “**RCO**”) is accountable for ensuring all staff are fully aware of the Company’s Privacy Policy. The RCO monitors compliance with the Policy and manages any Policy breaches (see section 10 below). Please note that the Company is not formally required nor chooses to nominate a *Data Protection Officer*.

3 **What does the Company use your personal data for?**

The Company processes very little personal data and only holds personal data for the following legitimate purposes:

1. To fulfil staff employment requirements (e.g. recruitment, payroll and performance reviews).
2. To enable client registration and access to the Securitisation Repository.
3. To maintain outsourcing and supplier contact details.

4 **What personal data does the Company collect?**

The Company only holds personal data where there is a legitimate purpose to do so and/or the consent of the individual has been obtained.

4.1 **Employees and Contractors**

The personal data maintained for employees and contractors is:

1. Name
2. Job title and role
3. Work contact details, including email addresses and telephone numbers
4. Personal contact details, including your personal email addresses and telephone number
5. Emergency contact information
6. Account login details, including username and password
7. Bank details
8. Employment and education history (CV information)
9. Copies of identity verification documentation (e.g. passport)
10. Information about your status in relation to your right to work/ work eligibility

4.2 **Securitisation Repository system users**

The personal data maintained about users of the Securitisation Repository system is:

1. Name
2. Job title and role
3. Work contact details, including email addresses and telephone numbers
4. IP address and location data.

4.3 **Outsourcing Contacts and Suppliers**

The personal data maintained about outsourcing contacts and suppliers of the Company is:

1. Name
2. Job title and role
3. Work contact details, including email addresses and telephone numbers

5 How confidential is your data?

The Company will keep all personal data confidential and will not share it with third parties without your consent, except in the following circumstances:

1. We are required by law to disclose it to a governmental or other authority.
2. We share it with parties that provide services to us and who are under obligation to keep the information confidential.
3. We may provide it to any party to which we transfer our rights and duties under any agreement with you.
4. We do not transfer your data outside the European Economic Area and the United Kingdom.

6 How secure is your data?

All personal data is held in an encrypted format and stored on a secure environment with agreed access controls. Any personal data held within the Securitisation Repository is anonymised and encrypted.

7 How long is personal data kept for?

The Company will keep personal data only for as long as it is needed for the purposes of the relationship and for a reasonable period after that relationship terminates in case of any issue arising in relation to the termination of the relationship.

8 Recording Company meetings

In certain circumstances, the Company may record Company meetings and training sessions – for more details, see attached “Guidelines to Recording Meetings”.

9 Rights in relation to the personal information held by the Company

All individuals who the Company holds information about have the following rights under the *General Data Protection Regulation* in relation to personal information held by the Company:

9.1 Subject Access Request

You are entitled to ask the Company for details about the personal data held about you. The request should include:

1. A title ‘Subject Access Request’.
2. The date of the request.
3. Name (including any aliases, if relevant).
4. Any other information used by the organisation to identify or distinguish you from other individuals (e.g. customer account number or employee number).
5. Your up-to-date contact details.
6. A comprehensive list of what personal data you want to access, based on what you need.
7. Any details, relevant dates, or search criteria that will help the organisation identify what you want.

The Company will respond to such a request promptly and, in any event, within one month of receipt, setting out details of the information about you that we hold, including:

1. The source(s) from which we acquired the information.
2. The purposes for which we process the information.
3. Any persons or entities with whom we share the information.

9.2 Right to Rectification

You are entitled to require us to correct any inaccurate personal data that we hold.

9.3 Right to Erasure

You may be entitled to instruct the Company to erase your personal data. If asked to erase personal data the Company must do so without undue delay, unless there is a compelling, lawful reasons not to.

9.4 Right to Restriction of Processing

You have the right to require the Company to restrict processing of your personal data where:

1. You have contested the accuracy of the personal data and its accuracy has not yet been verified.
2. The processing is unlawful, and you oppose the erasure of your personal data and instead request restriction of its use.
3. The Company no longer needs the personal data, but it is required by the data subject for the purpose of making or defending legal claims.

9.5 Right to Data Portability

You have the right to receive your personal data in electronic format and to request that it is transferred to a third party.

9.6 Right to Object

You have the right to object to the processing of your personal data. If you do so, the Company will stop processing that personal data unless it can demonstrate compelling legitimate grounds to do so.

10 Accuracy of Personal Information

The Company will take all reasonable steps to ensure that all personal information held is accurate and up to date.

11 Data security breaches

An information security breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, electronic or physical data. It includes breaches that may be the result of both accidental and deliberate causes. Information security breaches can include:

1. Access to data or systems by an unauthorised third party.
2. Deliberate or accidental action (or inaction) by any person to interfere with data or systems.
3. Sending data to an incorrect recipient.
4. Computing devices and documents being lost or stolen.
5. Alteration of data or systems without permission.
6. Loss of availability of data or systems.

Any breach of information security must be reported immediately to the RCO who will assess the materiality of the breach and determine the appropriate response in compliance with GDPR and any other relevant legal requirements.

12 Special Categories of Personal Data

Under the GDPR, personal information about the following are deemed to be “special categories” of personal data:

1. Race/ethnicity
2. Political views
3. Religious/philosophical beliefs
4. Trade Union Membership
5. Sex life/orientation
6. Genetics/biometrics
7. Health/medical information

The Company will not hold any personal data relating to these categories.

13 Who to contact about your Personal Data

Any individual who:

1. Has questions about how the Company deals with their personal data
2. Wishes to invoke one or more of their rights outlined in Section 9 above, or
3. Has a complaint about the Company's use of their personal information

Should contact the Company's Risk and Compliance Officer at dataprotection@secrep.eu.

14 Complaint to Supervisory Authority

If we cannot resolve your complaint to your satisfaction you may wish to make a formal complaint to the Dutch Data Protection Authority (<https://autoriteitpersoonsgegevens.nl/nl>).

15 Changes to this Policy

We will regularly review this Policy and may change and update it as we consider appropriate. However, we will not significantly change how we use your personal information without your consent.

Attachment - Guidelines for Recording Meetings

1. Recording Meetings

Recording or transcribing a meeting at SecRep BV (the '**Company**') will, in principle, only be permitted when it relates to the following:

- a Supervisory Board meeting;
- a Risk and Controls Committee meeting;
- a formal Management Board meeting;
- training;
- by exception, when the nature or subject matter of the meeting (including, for the avoidance of doubt, an external meeting) and by implication a precise, comprehensive and accurate record of the discussion, justifies the recording thereof.

In addition to the type of meeting potentially recordable, recording is only permitted where the undermentioned criteria/conditions are met/fulfilled. The tool/platform used to record meetings should be configured in line with the Company's Record Keeping Policy and Procedures (Annex 112).

2. Prescribed procedures prior to the Meeting

1. **Purpose:** Recording a meeting must have a specific, agreed-upon purpose which shall be set out in the invitation.
2. **Usage:** Recordings and transcripts may only be used for this specific purpose.
3. **Allowed Purposes:**
 - o To assist the minute-taker in documenting statements as required by law, regulations or Company practice;
 - o To help participants who attend the meeting to check the minutes. (e.g., in decision-making or information dissemination); or
 - o To facilitate training and education.
4. **Notification:** If a meeting is recorded or transcribed, this should be noted in the digital invitation for example "For the purpose of minute-taking, a recording or transcript will be made of this meeting."

3. At the Start of the Meeting

The person starting the recording (usually the chairperson or minute-taker) shall note the meeting is to be recorded (and repeat this for recurring meetings) and explain the purpose therefor.

4. During the Meeting

The person starting the recording (usually the chairperson or minute-taker) shall:-

- commence doing so only after announcing it and after getting approval from all participants. Passive participation does not constitute consent;
- assume the responsibility for handling the recording properly, including after such meeting; and
- stop recording immediately if any participant requests it. Resume only with renewed consent.

5. After the Meeting

The person starting the recording (usually the chairperson or minute-taker) shall:-

- note in the minutes that all participants gave explicit consent for recording or transcription;
- share recordings and transcripts only with meeting participants or additional parties as can be agreed with participants in advance and only for the stated purpose, upon request; and
- delete recordings and transcripts once they are no longer needed in accordance with the Company's Record Keeping Policy and Procedures (Annex 112).