SCEU Group Rule	Employee Personal Data Rule	R-F-12
Human Resources		May 2018

EMPLOYEE PERSONAL DATA RULE

Contents

Applying the SCEU Data Protection Rule 3
Definitions 3
Purpose, Scope and Responsibility 3
General 3
Lawful basis 3
Purpose Limitation: 4
Privacy Notice 4
Confidentiality and integrity 4
Individual rights and requests 5
Sensitive Personal Data 5
Processing Employee Personal Data for recruitment and selection 5
Advertising 5
Application forms 5
Verification and Vetting 6
Applicant Screening and "Short-listing" 6
Interviews 6
Recruitment Records 6
Processing Employee Personal Data for personnel management 6
Time and attendance records 7
Sickness, disability and injury records 7
Pension and insurance schemes 8
Equal opportunities monitoring 8
Discipline, grievance and dismissal 8
References 8
Processing Employee Personal Data for operations management 9
Merger, acquisition and business re-organisation 9
Publishing Employee Personal Data 9
Processing Employee Personal Data for security management 10
Fraud detection 10
Sharing Employee Personal Data with others 10
Data exports outside the EEA 10
Requests from law enforcement or other competent authorities for Employee Personal Data 11
Sharing Employee Personal Data within the Sumitomo Corporation Group 11
Sharing Employee Personal Data with third parties 12
Request from Individuals 13
Schedule 1: Key Terms and Definitions 15

Applying the SCEU Data Protection Rule

Definitions

SCEU HR Human Resources and Facilities Department.

Manager Can include the Line Manager, Assistant Manager or Department General Manager where appropriate.

Purpose, Scope and Responsibility

The purpose of this Rule is to provide practical advice on how to apply the Data Protection Rule in the context of employment.

This Rule applies to everyone working for SCEU Group Companies subject to GDPR (i.e. establishment in the European Union or processes Personal Data in respect of any Employee in the European Union).

This Rule does not apply to the Processing of other Personal Data, such as customer or business contact Personal Data, which falls under the Business Personal Data Rule and the Rule for sharing Company Personal Data with Third Party Service Providers.

Failure to comply with this Rule can legally expose SCEU Group as an organisation and may result in disciplinary action against you. If you become aware of a breach or potential breach of this Rule, you should immediately contact the Data Protection Manager and SCEU HR as the Company is under strict timeframes to respond to breaches and may be subject to heavy fines.

SCEU HR is responsible for the content of this Rule and may update this Rule from time to time without notice to you. It is your responsibility to check back regularly for updates. This Rule was last updated on 22 May 2018.

This Rule is subject to any additional requirements of local law.

If you have any queries regarding this Rule, you should contact the SCEU HR department.

General

Lawful basis

Any Processing of Personal Data requires a lawful basis to be compliant with Data Protection Law, this basis includes where the processing is:

- necessary for the performance of the employment contract;
- required by law;
- in the employer's Legitimate Interests which outweigh the general privacy rights of employees (and a Legitimate Interest Assessment has been carried out); and
- done with consent (which must be given freely).

Any Personal Data deemed to be irrelevant or excessive should not be obtained or, where the Personal Data has already been obtained, should be destroyed in a secure and appropriate manner.

Information collected should only be retained for as long as is necessary. The Company may need to retain some information to protect its legal position, but this does not necessarily mean the entire record must be kept indefinitely. Please refer to the Preservation Period of Documents Rule for more information.

Purpose Limitation

At any stage of the recruitment, selection and employment, only collect Employee Personal Data that is adequate, relevant and not excessive, having regard to the purpose for which it is processed. Do not collect Employee Personal Data simply because it may be useful later on.

Privacy Notice

- When obtaining Employee Personal Data, either from the Individual or indirectly, you should make a Privacy Notice available. The Privacy Notice should include, as a minimum:
    - the identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative (e.g. SCEU Group Company or a third party) and of the data protection officer, where applicable;
    - the purpose(s) for which the Personal Data is intended to be Processed as the legal basis for the processing (including the legitimate interest relied on if applicable);
    - the recipients or categories of recipients of the Personal Data, if any;
    - where applicable, the fact that the Data Controller intends to transfer Personal Data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; and
    - where Personal Data has not been obtained directly: categories of Personal Data concerned, retention period and criteria, existence of Individual rights (including access rights, right to withdraw consent and lodge a complaint, source of Personal Data and the existence of automated decision-making).
- A further Privacy Notice should be provided to the Individual if, after the Employee Personal Data is collected, you intend to Process it in a significantly different manner to that made known at the time.
- When Personal Data is collected indirectly (for example, we obtain it from a third party or publically available source), we must seek to ensure that any third party provides appropriate Data Protection Law guarantees and we should send our Privacy Notice to such Individuals as soon as possible on obtaining the Personal Data (in any case on first communication with the Individual) unless it is impossible or requires a disproportionate effort.
- The SCEU Employee Privacy Rule can be found on the intranet.

Confidentiality and integrity

- Apply appropriate security measures to protect Employee Personal Data depending on its nature and sensitivity and the risks of unauthorised access, accidental loss or destruction or damage to the

records and anonymise Employee Personal Data where practicable. Security measures can be physical (e.g. secure cabinets), technical (e.g. passwords, encryption) and organisational (e.g. access controls, audit trails).

- All Employees involved in selection, recruitment and/or Employee Personal Data processing in the SCEU Group must have received appropriate training.

Individual rights and requests

- Individuals have a number of rights in respect of their Personal Data and the Company is under obligation to comply when the conditions are met and under strict timeline (see below and Data Protection for more details).
- Where reasonably practicable, provide Individuals with access to correct their own Employee Personal Data online.
- Allow Employees to check their own records periodically to correct mistakes and update any Personal Data.

Sensitive Personal Data

- Ensure you have a lawful basis in respect of Sensitive Personal Data which are stricter and narrower than for other types of Personal Data (i.e. strictly necessary to comply with laws or with explicit consent).
- Consider and use measures to process Sensitive Personal Data in an Anonymised or Pseudonymised form to the fullest extent possible.

Processing Employee Personal Data for recruitment and selection

Advertising

- SCEU Group's job advertisements should identify the Company or recruitment agency to which an Individual will provide his/her Employee Personal Data.
- The relevant SCEU Employee Privacy Rule should be sent to candidates at the earliest convenience after receiving an application or any Personal Data.
- Where recruitment is for a range of vacancies, rather than a specific role, SCEU Group should make this clear at the earliest opportunity.

Application forms

- SCEU Group's application forms shall only collect Employee Personal Data necessary to assess Individuals for the post for which they apply.
- In particular, collection of Employee Personal Data about criminal convictions shall be considered very carefully and minimised as much as possible. It shall only be sought where the appointing Company determines it is strictly necessary in respect of the role envisaged, where it has a lawful basis and only where permitted by applicable law.
- Other categories of Sensitive Personal Data should not be collected unless strictly necessary and the Processing is permitted by and in accordance with applicable law.

Verification and Vetting

- SCEU Group may validate Employee Personal Data provided by Individuals during the recruitment process ("Verification") and/or collect Employee Personal Data from third parties other than the Individual ("Vetting"). Where this occurs:
    - Individuals should be told in advance which aspects of their Personal Data will be Verified and if any Vetting will take place, including an explanation of how the Vetting or Verification will be carried out, including details on any third parties which may receive or provide Employee Personal Data;
    - information about criminal convictions (if collected) will only be collected through official authorised sources and in accordance with applicable law;
    - SCEU Group shall only contact a third party to complete any Verification or Vetting if the Individual has been informed and SCEU Group has a lawful basis to proceed; and
    - SCEU Group should give Individuals the opportunity to explain any discrepancies which emerge or any information uncovered which has an adverse effect on their application.
- Any Vetting should also:
    - be restricted to roles where it is genuinely necessary;
    - not involve approaches to colleagues or family of Individuals, except in exceptional circumstances; and
    - be targeted at the collection of specific and not general information.

Applicant Screening and "Short-listing"

- SCEU Group should short-list and screen applicants on consistent criteria and in compliance with applicable local laws,

Interviews

- SCEU Group shall only collect relevant information from Individuals at any interview.
- All interview notes shall be stored securely.

Recruitment Records

- SCEU Group shall securely store Personal Data collected from unsuccessful candidates. Such information should be destroyed after 6 months unless there is a genuine business reason not to. For example, an Individual's details might be kept for consideration for future positions, if their Consent is given for this.

Processing Employee Personal Data for personnel management

Personnel management typically includes activities related to the maintenance and termination of employment relationships. This may include performance assessment, attendance monitoring and training, payroll and administration of Employee-related benefits and insurance schemes, handling grievances or

disciplinary actions, business trip travel and overseas assignments, absence management and providing references.

Time and attendance records

- A SCEU Group Company may Process a limited amount of Biometric Personal Data from Employees as part of a Touch ID system to record time and attendance. Biometric Personal Data is Sensitive Personal Data and its processing is based on Consent. This Consent may be withdrawn at any time by the Employee therefore procedures should be in place to allow for such requests to be effected in a timely manner and a suitable alternative to be put in place.
- Biometric Personal Data shall only be accessed by SCEU HR and shall not be used for any purpose other than the recording of Employee absences and the time of clocking in and out by an Employee.
- The Touch ID system shall generate reports on non-attendance or late entrance and send these to the relevant managers. Reports and information shall not be shared with any other Department, SCEU Group Company or third party.
- The Touch ID system scans the Employee's Biometric Personal Data (a fingerprint) and converts the scan into a mathematical representation, creating a finger scan template, which is then stored in an encrypted format. As a result, no actual Biometric Personal Data shall be stored. Instead, digital profile characteristics are stored securely to compare against a newly offered set of characteristics for verification.
- Biometric Personal Data shall not be used or accessed for any purpose other than time and attendance records. Employees shall be notified and must consent to their Biometric Personal Data being used for any other purpose.
- As soon as an employee leaves the workplace, their Biometric Personal Data shall be immediately deleted.

Sickness, disability and injury records

- Sickness, disability and injury records, together with other health Personal Data which include information about an Individual's mental or physical health are Sensitive Personal Data will only be processed where:
    - there is a legal obligation to do so under employment and social security and social protection law preventive or occupational medicine or for the assessment of the working capacity of the Employee;
    - it is necessary to protect the vital interest of an Individual where the data subject is physically or legally incapable of giving Consent;
    - it is necessary for the defence of legal claims; or
    - the Individual has given explicit consent to the disclosure.
- Access to these records should be strictly limited to staff who have a legitimate business need to know and appropriate training. Security measures should be taken to this effect.

Pension and insurance schemes

- If Employee Personal Data is required by a third party to administer a scheme, the information must not be accessed or used for general employment purposes. For example, an Individual's medical report needed for a pension scheme may not be used in connection with decisions about the Individual's eligibility for sick pay.
- Limit your exchange of Employee Personal Data with a scheme provider to the minimum necessary for the operation of the scheme.

Equal opportunities monitoring

- Employee Personal Data collected for equal opportunities monitoring may include Sensitive Personal Data. Therefore, make sure that such information is not used for any other purposes.
- Ensure questions are designed so that the Employee Personal Data collected is accurate and not excessive. For example, do not limit the range of answers regarding ethnic origin so Individuals can make a choice that properly describes them.
- Consider and use measures to process any such Sensitive Personal Data Anonymised or Pseudonymised to the fullest extent possible.

Discipline, grievance and dismissal

- Ensure all records used in the course of disciplinary and grievance proceedings are accurate and sufficiently detailed to support any conclusion drawn about the Individual from them.
- Ensure these records are kept securely and only made available to authorised persons. For example, where information is to be provided to an employee representative or legal advisor, you should check that this person has been authorised by the Individual to act on his or her behalf.
- Do not access or use Employee Personal Data already kept because it may have some relevance to a disciplinary or grievance investigation. This would be incompatible with the purposes for which this information was obtained.
- Ensure that when employment is terminated the reason for this is accurately recorded and the record accurately reflects what the Individual has been told about the termination.

References

- Corporate references may only be given bySCEU HR.
- Confidential references should not be provided unless it is clearly the Individual's wish.
- When responding to a request from an Individual to see his or her own reference where the reference enables a third party to be identified, such as a colleague, it should be assessed whether it is lawful to transfer or withhold such Personal Data (e.g. if the named individual's Consent has been obtained).

Processing Employee Personal Data for operations management

Operations management typically includes activities related to managing SCEU Group's business operations, such as deploying Employees on projects, scheduling work, managing company assets and liabilities and publishing Employee Personal Data in directories, websites, annual reports and other publications.

Where possible, consider and use measures to process Anonymised or Pseudonymised Personal Data to the fullest extent possible.

Merger, acquisition and business re-organisation

- Ensure that, to the extent practicable, disclosure of Employee Personal Data is limited to Anonymised details. Employee Personal Data may only be disclosed in a non-anonymised format in limited situations where it is strictly necessary for the evaluation of assets and liabilities or the business re-organisation.
- Where Employee Personal Data is to be disclosed, obtain assurances from the receiving entity by using adequate data protection binding contracts (please refer to the Rule for sharing Personal Data with Third Party Service Providers and/or any applicable intra-group data transfer agreement). In particular, the Company shall seek to ensure that the Employee Personal Data disclosed will:
    - be treated in confidence;
    - not be further disclosed to other parties;
    - be used solely for the purpose of the disclosure; and
    - be destroyed or returned after its use.
- Where the disclosure of Employee Personal Data in respect of the operation envisaged involves the transfer of Employee Personal Data to another organisation outside of the EEA, the relevant SCEU entity shall ensure to be using adequate safeguards in respect of such international transfers of Employee Personal Data
- Where Processing Personal Data about new Employees acquired as a result of a merger, acquisition or re-organisation, make sure that the records are accurate, relevant and not excessive.
- Provide Employees with a Privacy Notice if their Personal Data is Processed outside of the nature and scope previously understood.

Publishing Employee Personal Data

- Employee Personal Data is often published as part of SCEU Group's business. For example, such Data is contained in annual reports, marketing materials, on websites and in directories.
- Unless there is a legal obligation to do so (e.g. in SCEU Group's annual reports), only publish Employee Personal Data if:
    - Anonymised or Pseudonymised Personal Data to the fullest extent possible;
    - It is in the Company's Legitimate Interest and is not overridden by Individuals' rights or potential harm (for example: a directory made available on the intranet); or

- the Individual has given his/her prior Consent.

- If an Individual decides to withdraw their Consent allowing the Employee Personal Data to be published, there should be an easy procedure for the Individual to request this and the Data should be removed promptly.
- Make sure that Individuals are offered a means to correct their Personal Data that has been published and to object to publication where it would cause significant damage or distress and informed of such rights.

Processing Employee Personal Data for security management

Security management typically includes activities related to ensuring the security of SCEU Group premises, assets, information, and Individuals. This includes monitoring the security of computer systems and networks, identifying and authenticating Employees and Individuals, establishing a network of emergency contacts, preventing fraud and other crime and ensure compliance with SCEU Group policies and Rules.

Fraud detection

Do not disclose Employee Personal Data for the prevention or detection of fraud unless:

- the disclosure is required by law;
- it is reasonably believed that failure to disclose in a particular instance is likely to prejudice the prevention or detection of crime; or
- Consent is obtained.

Sharing Employee Personal Data with others

Data exports outside the EEA

In respect of any international transfer of Personal Data, regardless of whether it is to a Sumitomo Group entity or a third party, Business Personal Data may only be transferred to an entity outside the EEA or to an international organisation if:

- Adequate safeguards are in place:
  - the recipient entity is processing Personal Data in a country which the European Commission has found to provide adequate protection for Personal Data; or
  - Individuals have given their explicit and informed Consent to the transfer; or
  - both entities have signed a data transfer agreement including clauses approved by the European Commission or supervisory authority; and
- Individuals have been informed of the purposes of the transfer, the recipients of the Employee Personal Data and that the countries may have different data privacy standards and have been given an opportunity to object;
- Unless the transfer is required by law, Individuals have given their explicit Consent to the transfer if it involves Sensitive Personal Data; and
- the transfer is otherwise permitted under applicable law.

Please contact the Data Protection Manager and SCEU Legal Department if you are transferring or intending to transfer Personal Data outside of the EEA.

Requests from law enforcement or other competent authorities for Employee Personal Data

- SCEU Group can disclose Business Personal Data when required by law or when it can rely on another lawful basis in accordance with Data Protection Law.
- You should immediately consult with the Data Protection Manager and SCEU Legal Department before responding to a request from the police or other authority including any supervisory authorities.
- If you receive a 'mandatory' request, you should not rely on the requestor's assurance that the disclosure is in fact mandatory. Instead, always ensure that the Data Protection Manager and the SCEU Legal Department have confirmed this internally. In some cases, SCEU Group may still have the discretion to decide whether to comply with the authority's request.
- If it is decided that you should disclose Employee Personal Data, you should only ever disclose the minimum amount necessary to achieve the requestor's specified purpose and keep a record of such disclosure unless unlawful.
- Where practicable and allowed under the law, Individuals should be told, about the disclosure, such as what Personal Data has been shared, who to and why.

Sharing Employee Personal Data within the Sumitomo Corporation Group

- You can share Employee Personal Data within Sumitomo Corporation Group if:
    - The relevant international transfer of data safeguards have been put in place (see Section 0 above) and the relevant data protection obligations and assurances have been provided for (see below and o below);
    - the Individual has been informed (this would usually be in the relevant SCEU Employee Privacy Policy or another Privacy Notice communicated to the Employee);
    - it is in the Company's Legitimate Interest which the Individual would reasonably expect (and is informed of); or
    - the Individual has given his/her Consent (necessary if sharing the Employee Personal Data may affect his/her privacy).
- You should only share the minimum amount of Employee Personal Data necessary to fulfil the request. Consider whether the information can be Anonymised or Pseudonymised before it is shared or whether any unnecessary data fields can be removed.
- Data sharing between Sumitomo Corporation Group entities as Data Controllers
- A Sumitomo Corporation Group entity may share Employee Personal Data with another Sumitomo Corporation Group entity if:
- the Employee Personal Data shall be used and Processed in a manner that is compatible with the purpose for which it was originally collected; and

- the Employee Personal Data is made available to representatives who have a clear 'need to know' in connection with their usual Sumitomo Corporation Group role, such as those in a managerial position with responsibility for the Individuals concerned or a Human Resources role. For example:
    - Where an Individual's job responsibilities span more than one country, Employee Personal Data may be transferred to managers and colleagues in those other countries;
    - Where an Individual's line manager is located in a different country, the Employee Personal Data may be transferred to such country in order to support that management relationship;
    - Where a member of the SCEU Group's Human Resources function has responsibility for Individuals from several countries, Employee Personal Data for Individuals working for Sumitomo Corporation Group in those countries or in that region may be made available to him/her.
    - Data sharing where one Sumitomo Corporation Group entity Processes on behalf of a Sumitomo Corporation Group entity
- One Sumitomo Corporation Group entity might provide a data Processing service to another Sumitomo Group entity, such as centralized storage of data or application hosting. When this occurs, the entity providing the Personal Data must:
    - use a Sumitomo Corporation Group entity providing sufficient assurances with respect to the technical and organisational security measures governing the Processing;
    - have entered into a binding contract with the recipient providing satisfactory compliance to Data Protection Law (i.e. an intra-group data transfer agreement); and
    - instruct the Sumitomo Corporation Group entity on how to Process the Employee Personal Data, requiring compliance with equivalent security and confidentiality obligations.
- The Sumitomo Corporation Group entity which Processes the Employee Personal Data shall do so in accordance with instructions and shall apply and maintain appropriate technical and organisational measures to protect against unauthorised access, accidental loss, damage or destruction, particularly when Employee Personal Data is transmitted over a network.

Sharing Employee Personal Data with third parties

Employee Personal Data may not be disclosed outside of Sumitomo Corporation Group, except where it is necessary:

- to protect an Individual's vital interests;
- when required by law;
- in the Legitimate Interest of the Company:
    - to engage a Third Party Service Provider;
    - where necessary for the establishment, exercise or defence of legal claims as directed by SCEU Legal Department;
    - to engage external auditors to validate SCEU Group's financial accounts;

- to engage professional advisers (e.g. bankers, lawyers, accountants, external auditors) and liaise with potential buyers and vendors in connection with the disposal or acquisition by SCEU Group of a company or a company's assets (please see Section 0 above);
- to administer SCEU Group's contractual relationship with organisations who provide "external workforce" to SCEU Group by disclosing relevant information about the Individuals provided (e.g. number of days worked of an agency employee); or

- for the performance of a contract with the Employee.

Individuals should be given a Privacy Notice that their Employee Personal Data is to be shared with third parties.

When engaging a Third Party Service Provider, consider the following:

- Due diligence – select a Third Party Service Provider providing sufficient guarantees with respect to data security and the handling of Employee Personal Data generally.
- Contractual obligations – ensure that the contract with the Third Party Service Provider includes specific data privacy obligations. The relevant contractual clauses will differ, depending on whether the Third Party Service Provider is engaged as a Data Controller or a Data Processor.
- Compliance monitoring – take reasonable steps to monitor the Third Party Service Provider's performance of the relevant security and Processing obligations.
- Transfers – if Employee Personal Data may be transferred to countries outside the EEA then additional safeguards must be taken to protect the Employee Personal Data (please refer to Section 0 above).
- Please refer to the SCEU Rule for sharing Personal Data with Third Party Service Providers for further details.
- Contact the Data Protection Manager and the SCEU Legal Department.

Request from Individuals

- Individuals have various rights under the Data Protection Law:
  - to information about what Personal Data is being Processed on them and for what purposes ;
  - to obtain from us access to Personal Data Processed by us concerning them;
  - to require that we rectify inaccurate Personal Data concerning them;
  - to require us to erase Personal Data concerning them where certain grounds apply;
  - to require us to restrict (i.e. to suspend) Processing of Personal Data where certain grounds apply;
  - to receive a copy of Personal Data concerning them in a machine-readable format and to have it transmitted to another data controller; and
  - to object to automated decision making.
- If you think you have received a request in respect of the right of an Individual under Data Protection Law (a "**Data Subject Request**") you should immediately contact the Data Protection

Manager and SCEU HR . A Company has an obligation to respond to such request within a month so escalating the query to the Data Protection Manager and SCEU HR as soon as possible is very important.

- The Data Subject Request may not apply to legally privileged information, information processed in respect of certain grounds or Personal Data about another person.
- You must not respond to a Data Subject Request directly. However, if an Individual is requesting specific Employee Personal Data about themselves which they have already received and has not indicated that this is a Data Subject Request, you may provide the information again. For example, if an Individual is merely asking for you to re-send a copy of an email which they previous received, there should be no problem with sending this to them.
- Please refer to the Data Protection Rule for further details.

Schedule 1: Key Terms and Definitions

Key Term	Definition
Anonymisation	Processing personal data in such a manner that the Individual is not or no longer identifiable. Anonymised data is therefore information which does not relate to an identified or identifiable Individual (i.e. it is not possible to identify an individual, directly or indirectly, from the data). Statistics are usually anonymised data.
Biometric Personal Data	personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images, fingerprints, the iris, retina, face, ears, DNA and typical posture and gait.
Company	The SCEU Group entity for which you are employed and/or perform your function.
Consent	The agreement of the Individual (which must be freely given, specific, informed and be an unambiguous indication of the Individual's wishes) by which they, by a statement or by a clear positive action, signify that they allow you to Process their Personal Data for the specific purpose or purposes communicated to the Individual.
Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data is, or is to be, Processed.
Data Processor	Any person, company or entity (other than an employee of the Data Controller) who Processes the Personal Data on behalf of the Data Controller.
Data Protection Law	All laws relating to data protection, privacy and security, including, without limitation: (a) EU Directives 95/46/EC and 2002/58/EC (the "**Directives**"), all national laws implementing the Directives; and (b) EU General Data Protection Regulation (EU) 2016/679 ("**GDPR"**), and/or any corresponding or equivalent national laws or regulations; and (c) any judicial or administrative interpretation of any of the above, and any guidance, rules, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant supervisory authority.
Data Protection Principle(s)	Data protection principle(s) set out in the SCEU Data Protection Rule.
Data Protection Rule	The most recent version of the SCEU Data Protection Rule document.
EEA	The European Economic Area which includes: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom
Employee	Individuals whose Personal Data may be collected and processed as part of the joining, being part or related to of the workforce of an SCEU Company, including but not limited to:

	(i) current and former SCEU Group employees (both permanent, temporary, part-time or full-time), including retirees; (ii) Individuals who, although not SCEU Group employees, are part of SCEU Group's "external workforce" such as consultants, independent contractors and temporary agency workers; (iii) job applicants and other prospective SCEU Group employees, such as those joining SCEU Group in connection with SCEU Group acquiring all or part of a third party's business; (iv) dependants and beneficiaries of current and former SCEU Group employees and Individuals who should be contacted in the case of an emergency, where such information is provided to SCEU Group by an employee in connection with his/her employment relationship with SCEU Group; or (v) students when engaged as part of their study or on work experience (e.g. internship) at an SCEU Group company.
Employee Personal Data	All Personal Data relating to an Employee collected and Processed by or on behalf of SCEU Group in an employment context and which may include without limitation: (i) contact details, such as an Employee's address, telephone number and email address, and the contact details of other Individuals, such as details of who to contact in the event of an emergency and details of the dependents and beneficiaries of an Employee; (ii) financial information relating to an Employee's compensation, benefits, pension and retirement arrangements, such as details of his/her salary, banking institution and account number(s), tax codes, tax identification number or other government identifier, business expenses, stock options, stock purchase plan, etc.; (iii) recruitment information, such as an Employee's Curriculum Vitae (CV) or resume, photograph, gender, date of birth, citizenship, application form, notes of job interviews, willingness to relocate, desired or current salary, third party references (if obtained and recorded), academic and professional qualifications, academic transcripts, psychometric test results (if relevant and permitted to be collected by local law), drug and alcohol test results (if relevant and permitted to be collected by local law), other health and fitness assessments etc.; (iv) employment administration information, such as employment and career history, termination details, absence and vacation records, hours worked, health and safety records, sickness records, accident reports, terms and conditions of employment, personal development reviews and performance appraisals, disciplinary actions, expenses, membership, talent management records, driver's licence details and associated documents, skills records, training records, records of projects Employees have worked on, passport, work visa and associated documents, etc.; (v) details of an Employee's whereabouts in SCEU Group locations to the extent recorded by SCEU Group's electronic card access systems and video monitoring systems; (vi) details relating to an Employee's use of SCEU Group assets, such as computers, telephones, etc. (where relevant and permitted to be collected by local law) including

	user IDs and passwords; (vii) details relating to the administration of Employee benefits, such as share purchase schemes, health insurance programs, and pension or retirement schemes, including information about an Employee's spouse, domestic partner, dependents, or other beneficiary. (viii) information with respect to the administration of and an Employee's use of a corporate credit card, or other purchasing card, including relevant transaction records; and (ix) information about an Employee's travel for SCEU Group business or where otherwise recorded in the travel management system, including details of bookings, tickets and receipts for travel, accommodation and other expenses incurred, and if relevant, location and contact details.
Individual	A natural person who is the subject of Personal Data (also referred to as a "data subject").
Legitimate Interest	Legitimate interests is one of the lawful basis for processing and it is likely to be most appropriate where a Company uses Personal in ways the relevant Individuals would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Legitimate Interest Assessment	There are three elements to the legitimate interests assessment (also referred to as LIA): (a) identify a Legitimate Interest; (b) show that the processing is necessary to achieve it; and (c) balance it against the individual's interests, rights and freedoms.
Personal Data	Data relating to an identified or identifiable natural person. This can include (but is not limited to) names, email addresses and other contact details, photographs, opinions expressed about an Individual, and records of customer interactions. It includes, but is not limited to, data or information which is stored electronically, on a computer, or in a manual format which is organised by an identifier (e.g. by reference to Individuals).
Privacy Notices	Separate notices setting out information that may be provided to Individuals when a Company receives Personal Data. These notices may take the form of general privacy statements applicable to a specific group of Individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose. Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an Individual can easily understand them. Also referred to as Fair Processing Notices or Privacy Policies.
Processing or to Process	Any operation or set of operations performed upon Personal Data (whether or not by automated means) such as collecting, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, erasure or destruction.
Pseudonymisation	Processing of Personal Data where the data cannot by itself identify an individual without the use of additional information. Pseudonymisation is only effective where such additional information is kept separately and is subject to technical and organisational measures to

	ensure the data does not identify an Individual or make an Individual identifiable. For example, using an ID code in the general processing of customer data and ensuring the details that would identify the ID code holder (such as name, position, etc.) are kept separate under tight security controls).
Sensitive Personal Data	Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or genetic or biometric data of information concerning an individual's health, sex life, sexual orientation and criminal convictions information[1] (this is sometimes referred to as 'special categories of data')
SCEU Group	SCEU Group means: (i) Sumitomo Corporation Europe Limited ("**SCEU**") London office; (ii) SCEU Branches, including Norway (Oslo & Stavanger), Prague, Warsaw and Milan; (iii) SCEU Location Business Departments, including Aberdeen and Baku (iv) SCEU Location Liaison Departments, including Ashgabat; (v) Sumitomo Benelux S.A./N.V; (vi) Sumitomo Deutschland GmbH; (vii) Sumitomo France S.A.S.; and (viii) Sumitomo Corporation Espana S.A. (***Note 1***- The entities mentioned in items (v), (vi), (vii) and (viii) are also called the Regional Companies, pursuant to Regional Company Rule R-G-2 (SCEU Group Organisation)). (***Note 2***- Business Line Companies (as defined in Rule R-G-2) are outside the scope of this Rule. Business Line Companies should follow their own company policy/rule/Rule with respect to data protection.)
Sumitomo Corporation Group	Active legal entities which are majority owned or controlled by Sumitomo Corporation.
Third Party Service Provider	A third party vendor or supplier to a Company that may have access to Employee Personal Data in the course of providing services to the Company.