Solidatus

Solidatus data protection policy

Version: 2.0

Date: 28 Aug 2020

Author: Philip A. S. Miller

Contents

1. Purpose

1.1 This document sets out Threadneedle Software Limited's ("Solidatus")'s policy on data protection. It provides an overview of data protection requirements and directs you to more detailed guidance as appropriate.

1.2 If you have any questions relating to this policy please contact Solidatus' Data Protection Officer via philip.miller@solidatus.com.

2. Background to this policy

2.1 The General Data Protection Regulation (GDPR), which though an EU law has been incorporated into UK law alongside a new Data Protection Act (DPA), establishes a framework of rights and duties which are designed to safeguard personal data. These are referred to in this policy as 'Data Protection legislation'. The legislation is underpinned by a set of six straightforward principles, which define how data can be legally processed.

2.2 These six principles are:

2.2.1 Personal data shall be processed fairly, lawfully and transparently.

2.2.2 Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes. There is an exemption for research data.
2.2.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
2.2.4 Personal data shall be accurate and where necessary kept up to date.
2.2.5 Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. There is an exemption for research data.
2.2.6 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.

2.3 The GDPR also sets out rights of data subjects relating to their personal data. These rights include:

2.3.1 the right to access
2.3.2 the right to rectification
2.3.3 the right to erasure (in certain circumstances)
2.3.4 the right to stop processing
2.3.5 the right to portability (in certain circumstances)
2.3.6 the right to object to marketing, and
2.3.7 the right to have human intervention with regards to automated processing, including profiling.

2.4 The GDPR sets out the conditions under which information can be transferred to countries outside the European Economic Area (EEA). These include adequacy, appropriate safeguards, binding corporate contracts and explicit consent, amongst others. The UK considers countries in the EEA to be adequate, but after the Brexit transition period, the UK may be considered an international country, so contracts may be required.

2.5 The Legislation defines both personal data and special categories personal data.

2.5.1 Personal data is any information that can identify a living individual and can include such items as home and work address, personal email address, age, telephone number and schools attended, and even photographs and other images.
2.5.2 Special categories personal data consists of racial/ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and information relating to legal proceedings and convictions.
2.5.3 Personal data comes under the categories of confidential or restricted information in the Information Classification Standard depending on the volume. Special categories personal data comes under the category of confidential information only in the Information Classification Standard.

2.6 The GDPR sets out certain lawful bases that must be satisfied to justify the holding or use of personal data. These are set out in Article 6 of the GDPR and include: contract; legal; vital interests, public duty, legitimate interests and consent. Special categories data requires that (an) additional lawful basis as set out in Article 9 of the GDPR. This lawful basis is recorded in Solidatus' Information Asset Register. Staff who are unsure what lawful bases apply to personal data they intend to process should seek advice from the Data Protection Officer.

3. Policy and guidance

3.1 Solidatus is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

3.2 This Policy and the further company guidance it refers to apply to all personal data processed for Solidatus' purposes, regardless of where it is held and, in respect of automatically processed data, the ownership of the equipment used.

3.3 Links to relevant company guidance are set out at the end of this policy. This list is not exhaustive.

4. Application of this policy

4.1 Solidatus holds personal information about individuals such as employees, clients and others, defined as data subjects in Data Protection legislation. Such data must only be processed in accordance with the Data Protection legislation. This Policy and Solidatus Guidance are written to ensure such compliance. Any breach of this Policy and/or Solidatus Guidance may result in Solidatus as the Data Controller (and in some cases individuals), being in breach of Data Protection legislation and therefore liable in law for the consequences of such breach.

4.2 Heads of Department and Service Leaders are responsible for ensuring that Solidatus complies with Data Protection legislation. All staff must ensure they have read and understand this Policy and Solidatus Guidance.

4.3 It is the responsibility of all users of personal data throughout Solidatus to ensure that personal data is kept securely. Personal data should not be disclosed to any unauthorised third party in any form, either accidentally or otherwise.

4.4 Any breach of or failure to comply with this Policy or Solidatus Guidance, particularly any deliberate release of personal data to an unauthorised third party, may result in disciplinary or other appropriate action.

4.5 Solidatus will continue to perform periodic audits to ensure compliance with this Policy and Data Protection legislation and to ensure that all guidance and support is kept up to date.

4.6 Any unauthorised access to or disclosure of personal data or other data security breaches should be reported to the Data Protection Officer and/or the Information Security Manager as soon as possible, using the email address philip.miller@solidatus.com.

4.7 Solidatus Secretary is responsible for ensuring that Solidatus community remain informed of their obligations under Data Protection legislation, with operational duties of advice and support devolved to the Data Protection Officer.

4.8 The Data Protection Officer is required by Data Protection legislation to report to the highest levels of management at Solidatus, which will normally be done through Solidatus Secretary.

4.9 Staff procuring cloud-based services or mobile apps storing personal data for Solidatus must check with the Information Security team that these meet the security requirements of Data Protection legislation.

4.10 Staff should not conduct profiling exercises without first conducting a data protection impact assessment. Should they accidently through manipulation of data sets find they have identified individuals, they should contact the Data Protection Officer. Profiling is defined in the GDPR as 'any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her'.

5. Handling of personal data by staff

5.1 Staff should only use personal data for a company-related purpose, with the knowledge and express consent of an appropriate member of senior management. The use of personal data should be limited to the minimum consistent with the achievement of objectives.

5.2 Any confidentiality or consent agreements should normally be signed off by Solidatus' Board For advice, contact the Data Protection Officer.

6. Access to data

6.1 The DPA gives data subjects a right to access to personal data held about them within a set timescale. Therefore, it is important that the Data Protection Officer be notified of any request to Solidatus for access to an individual's personal data as soon as they are received.

6.2 There are specific provisions which apply to examination marks and comments.

6.3 Requests from police must be handled so that one or more senior managers within Solidatus must authorise the release of any data, prior to that release taking place. Full records must be kept of any data releases made to third parties, including the process of authorisation of such releases.

6.4 If you have any questions relating to access to personal data please contact the Data Protection Officer.

7. Retention of data

7.1 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. Solidatus' retention schedule outlines the length of time various classes of records and other data should be kept. This extends to backups and copies made on removable media.

7.2 Passport data and other immigration documents can only be collected via Solidatus' photocopiers/scanners by the relevant staff in Human Resources or the Executive who are required to keep copies for Visa purposes. These scans should only be kept for as long as we need to prove to UKVI that staff and interns have or had the right to be at Solidatus.

8. Data transfer

8.1 If data is being sent outside the European Economic Area by Solidatus, Solidatus needs to put in place certain safeguards. Please contact the Data Protection Officer if for any reason related to Solidatus, as part of a supplier contract or for your studies, for example, you may need to send personal data outside the EEA.

8.2 Information published on the web must be considered to be an export of data outside the EEA.

8.3 No web-based, or 'Cloud' services, storing personal data outside the EEA should be used for storing or sending special categories personal data unless this has been agreed with the Data Protection Officer.

8.4 Any transfers of personal data outside the EEA and/or extraordinary transfers of data should be signed off by Solidatus Secretary, unless to countries that are covered by an EU adequacy decision.

9. CCTV and physical access control

9.1 CCTV at Solidatus will be used in line with best practice on the use of CCTV.

9.2 Access control systems are used at Solidatus for the purposes of security, maintenance of IT and building systems and public safety.

9.3 Requests for information held within CCTV and access control systems made by police services under the relevant exemptions in Data Protection legislation will be handled by Solidatus' Security Office.

9.4 Requests for information held within CCTV and access control systems made by any other individuals or organisations will be handled by the Data Protection Officer.

10. Information Asset Register

10.1 Solidatus Information Asset Register (IAR) will be used to meet the record keeping requirements of Data Protection legislation.

10.2 Information Asset Owners, defined as the staff member with responsibility for the information asset, will ensure that they create and maintain the data held within the Information Asset Register.

10.3 This will include an annual review of their information assets.

10.4 The Data Protection Officer will ensure that Information Asset Owners receive the appropriate support to maintain the information asset register.

11. Compliance, policy awareness and disciplinary procedures

11.1 The loss or breach of confidentiality of personal data is an infringement of Data Protection legislation and may result in criminal or civil action against Solidatus. Therefore, all users of personal data at Solidatus' information systems must adhere to the Data Protection Policy and its supporting policies as well as the Information Security Policy.

11.2 All current staff, contractors and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

11.3 Any breach of this policy will be handled in accordance with all relevant Company policies.

12. Status of this policy

12.1 This Policy has been approved by the Information Governance Committee on 28th May 2018.

12.2 Other guidance will be made available to staff as developed. The approval process will include the Board.

Solidatus

Document control

Review schedule

Review interval	Next review due by	Next review start
3 years	May 2021	November 2020

Version history

Version	Date	Approved by	Notes
V1	28/05/2018	Board	
V2	28/08/2020	Board	Updated pre Cyber Essentials Audit

Links

Reference links	Link
General Data Protection Legislation	https://gdpr-info.eu/
Information Commissioner's Office	https://ico.org.uk/
Information Commissioner's Office Guidance on Cloud Computing	https://ico.org.uk/your-data-matters/online/cloud-computing/
Register of Data Controllers	https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

Contacts

Position	Name	Email	Notes
Data Protection Officer	Philip Miller	philip.miller@solidatus.com	Author

Communications and training

Action	Response
Will this document be publicised through Internal Communications?	Yes
Will training needs arise from this policy?	TBC
If 'Yes', please give details:	

Solidatus