Data Protection Policy

Overview

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Our Commitment (Policy Statement)

We are committed to the protection of the rights of individuals whose personal data we collect and process as part of delivering our services/products. We have developed this policy so we can describe in simple terms how we do this in line with all relevant laws and regulations, including the General Data Protection Regulation (GDPR). This policy has been made freely available so all interested parties can easily understand how we protect the data under our care. Our approach to managing personal data is reviewed on at least an annual basis to ensure it meets with the appropriate laws and regulations, and to ensure we are satisfied it provides adequate protection to personal data.

Our Privacy Notice lays out the personal data we collect and for what purpose:

- We only ever collect the minimum required information to achieve the identified purpose. We will not use personal data obtained for a specified purpose in any other way than that declared in our Privacy Notice and/or consented to by the owner of said data.
- Before we process personal data we will always identify a lawful basis for doing so, and we will provide clear, understandable and accessible information (e.g. a privacy notice displayed on our website) to help ensure all interested parties are as informed as possible and our processing of personal data is both fair and transparent.
- We will only retain data for as long as is necessary, and anonymise personal data wherever possible.
- The rights of Data Subjects (as defined in our Privacy Notice) in regards to the processing of personal data are fully supported at all times.

The scope of this Policy

This policy applies to all processing of personal data, including but not limited to processing personal data of:

- Potential and existing customers
- Potential and existing employees
- Potential and existing suppliers
- Partner organisation personal data

All of our employees, partner organisations (including our supply chain partners) and any third parties working with or for us, will be expected to read, understand and adhere to this policy. No third party may access personal data held by SharpStream Ltd without having the appropriate confidentiality/data processing agreement in place, which will mirror the conditions of this policy.

Key Roles and Responsibilities

We are identified as a both Data Controller and Data Processor under the GDPR.

Senior management and all those in managerial or supervisory roles throughout SharpStream are responsible for developing and encouraging good information handling practices, with specific responsibilities laid out in individual job descriptions.

Our Data Protection Representative has the following responsibilities (in line with Article 39 of the GDPR):

- To inform and advise our senior management and employees about our obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, and with our data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- To advise on, and to monitor, data protection impact assessments;
- To cooperate with the supervisory authority; and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc), specifically being the point of contact for data subject requests.

Those who have a specific responsibility to oversee the management of personal data are responsible for making sure this is done in line with this policy and supporting procedures.

Accuracy of Personal Data

We will make every reasonable effort to ensure the personal data we hold is accurate, including clear instructions for data entry, collecting minimal data to reduce the overall potential for error, and where possible putting controls around data entry fields to minimise the ability to enter inaccurate data.

Where inaccuracies are identified or changes are required, we have outlined a 'Right to Rectification' procedure (see 'Right to Rectification' Procedure). The specific Data Manager is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests.

Security of Personal Data

We do everything we can to secure personal data. All of our employees are responsible for ensuring that personal data we hold is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by us to receive that information and has entered into an appropriate data processing/confidentiality agreement. We risk assess the processing of personal data on at least an annual basis, or when a new requirement is identified. These risk assessments are carried out to minimise both the possibility and impact of a data security breach, and therefore minimise the threat to individual's privacy. The results of these assessments inform the security arrangements we put in place to protect personal data, a number of which are listed below:

- Password protection
- Automatic locking of idle terminals
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation
- Identifying appropriate international security standards relevant to SharpStream
- The appropriate training levels throughout SharpStream

- Measures that consider the reliability of employees (such as references, right to work checks etc.)
- The inclusion of data protection in employment contracts
- Identification of disciplinary action measures for data breaches
- Monitoring of staff for compliance with relevant security standards
- Physical access controls to electronic and paper based records
- Adoption of a clear desk policy
- Storing of paper based data in lockable fireproof cabinets
- Adopting clear rules about passwords
- Making regular backups of personal data and storing the media off-site
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

Personal data will only be deleted or disposed of in line with the Retention of Records Procedure.

Data Retention

Retention periods for personal data relating to specific purposes are laid out in our Privacy Notice and have been assessed based on perceived need. Personal data will be retained in line with our Retention of Records Procedure and destroyed securely following expiry of the retention period (see Retention of Records Procedure).

Any exceptions to the procedure must be documented clearly and agreed by the Data Protection Representative.

Disclosure to Third Parties

In order to provide the appropriate level of service we may need to share some personal data with third parties. These arrangements are summarised in our Privacy Notice and detailed in our Information Inventory. This sharing will only be for the specific purposes agreed, and will be carried out under the appropriate data processing /confidentiality agreements.

We will only transfer data outside of the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') when the appropriate safeguards are in place. These include:

An Adequacy Decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union:

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

In making an assessment of adequacy, we take account of the following factors:

- The nature of the information being transferred;
- The country or territory of origin, and final destination, of the information;
- How the information will be used and for how long;
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- The security measures that are to be taken as regards the data in the overseas location.

Privacy Shield

When transferring personal data from the EU to an organisation in the United States we check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce (US DOC). The obligations applying to companies under the Privacy Shield are contained in the “Privacy Principles”. The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their “membership” to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Binding Corporate Rules

If required we may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the Information Commissioner (relevant supervisory authority) for approval of these rules.

Model Contract Clauses

We may adopt approved model contract clauses for the transfer of data outside of the EEA. In this case we will adopt the model contract clauses approved by the (Information Commissioner's Office/ relevant supervisory authority) there is an automatic recognition of adequacy.

Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the Data Subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

Information Inventory

To ensure we have a clear view of risk to personal data, we have mapped where it sits within our organisation or is processed by our partners and assessed the level of risk associated. This data inventory and data flow determines:

- Business processes using personal data;
- Source of personal data;
- Volume of data subjects;
- Description of each item of personal data;
- Processing activity;
- Maintains the inventory of data categories of personal data processed;
- Documents the purpose(s) for which each category of personal data is used;
- Recipients, and potential recipients, of the personal data;
- The role of SharpStream throughout the data flow;
- Key systems and repositories;
- Any data transfers; and
- All retention and disposal requirements.

Note: This is summarised in our Privacy Notice.

Where there are changes to the type of processing, for example exploiting new technology or making changes to the approach, a further risk assessment will be carried out.

How SharpStream demonstrates its Compliance with the GDPR

We aim to be as effective and transparent as possible in how we manage personal data. We have documented and implemented this policy along with key supporting procedures so our approach is clear to interested parties. We also record the processing of personal data, and perform annual reviews to ensure the appropriateness of our approach.