General Data Protection Regulation (GDPR)

Issue date: December 2021 Issue: 02

Responsibility: Elserv Limited Directors

Purpose

This policy sets out how we seek to protect personal data and ensure that employees understand the rules governing the use of personal data. This policy requires employees to consult with their relevant management team member before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The company Directors has overall responsibility for this policy, with a data protection team representing each operating company having responsibility for the day-to-day implementation.

Definitions

- Data Subject: A data subject is the person to whom the data relates
- Personal Data: Any information relating to an identifiable person who can be directly or indirectly identified, particularly by reference to an identifier.
- Special Category Data: (sensitive data) The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
- Data Controller: A controller determines the purposes and means of processing personal data.
- Data Processor: A processor is responsible for processing personal data on behalf of a controller

Policy

Fair and lawful processing

Personal data must be processed fairly and lawfully in accordance with individuals' rights. This generally means data should not be processed unless there is a legal basis to allow it. For Elserv the lawful basis is one of the following

- Legal requirement
- Contract
- Legitimate Interest
- Consent
-

Responsibilities of Data protection team.

- Keeping the Directors updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all employees and those included in this policy.

- Answering questions on data protection from employees, board members and other stakeholders.
- Responding to individuals such as customers and employees who wish to exercise their rights under GDPR.
- Checking and approving data processing contracts or agreements for suppliers / contractors who handle the company's data.

The data protection team comprises of department heads.

Privacy Notice - transparency of data protection

We publish and maintain a privacy notice to data subjects.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees.
- Highlights that we may be required to give information to third parties such as expert witnesses and other professional advisers.
- Identifies that data subjects have certain rights over the data that we hold about them.

We strive for transparency in providing accessible information to individuals about the use of their personal data.

Conditions for processing

We ensure any use of personal data is justified using at least one of the conditions for processing and this is specifically documented. All employees who are responsible for processing personal data are aware of the conditions for processing. The conditions for processing are available to data subjects in the form of a privacy notice.

Rights of Data Subjects.

Personal data is only processed in recognition of the following rights

1. a right of access to a copy of the information comprised in their personal data;
2. a right to object to processing that is likely to cause or is causing damage or distress;
3. a right to prevent processing for direct marketing;
4. a right to object to decisions being taken by automated means;
5. a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
6. a right to claim compensation for damages caused by a breach of GDPR.

Sensitive personal data

In most cases where we process sensitive personal data, it requires the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent clearly identifies what the relevant data is, why it is being processed and to whom it will be disclosed.

Consent

Unless there is a legitimate reason to collect data in order to fulfil a legal contract, sensitive personal data is only collected with explicit active consent by the data subject. This consent can be revoked at any time.

Accuracy and relevance

We ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask for any inaccurate personal data relating to them to be corrected.

Your personal data

Employees must take reasonable steps to ensure that personal data held is accurate and updated as required. For example, if personal circumstances change, the employee can complete the change of details form and pass to department head.

Criminal record checks

We will conduct criminal record checks only when this is permitted by law. Criminal record checks do not necessarily require the consent of the subject

Data security

Details are covered in the IT procedure.

Privacy by design and default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. All system projects, involving personal data, have a requirement for a Privacy Impact Assessment.

Transferring data internationally

N/A

Data retention

Personal data is retained for no longer than the purpose it was originally obtained for. The retention period is defined on the data register. It is then deleted or securely archived.

Subject access requests

Upon request, a data subject has the right to receive a copy of their data in a structured format. Subject access requests must be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to a Third Party. This is completed at no cost to the data subject.

When a ‘subject access request’ is received, the employee should refer the request immediately to the Company Secretary.

Employees should contact their department heads if they have any concerns. Please note that there are restrictions on the information to which the employee is entitled to under applicable law.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

The Rights of Individuals to object to Direct Marketing

Employees should abide by any request from an individual not to use their personal data for direct marketing or profiling purposes and notify the Data Protection Team (department head) about any such request.

Direct marketing material should not be sent to someone electronically (e.g. via email) unless they have given consent.

Please contact the Data Protection Team (department head) for advice on direct marketing before starting any new direct marketing activity.

Reporting breaches

All employees have an obligation to report actual or potential data protection compliance failures to the Data Protection Team. This allows Elserv to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures, where these failures create a risk to the individual data subjects.
- Notify individuals if the breach causes a high risk to them

Full details for managing a Data Breach is published in the IT procedure.

Training

Employees in relevant roles receive suitable training on this policy. Training is refreshed periodically or if there is a substantial change in the law, policy or procedures.

Training covers:

- The law relating to data protection
- Elserv's data protection and related policies and procedures.

The completion of training is compulsory for all relevant employees.

Consequences of failing to comply

Elserv takes compliance with this policy very seriously. Failure to comply puts the business and employees alike at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under Disciplinary Procedure, which may result in dismissal.

If you have any questions or concerns about this policy, please do not hesitate to contact the Data Protection Team (Department head).

Ryan Smith
Director