SCREEN TECHNOLOGIES LIMITED

DATA PROTECTION POLICY

Context and Overview

Key Details	
Policy prepared By	Managing Partner
Approved by Board/Management	15/6/17
Policy became operational on	01/7/2017
Next review date	31/7/2020

INTRODUCTION

Screen Technologies Limited needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organization has relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards- and to comply with the law.

Why this policy exists

This data protection policy ensures Screen Technologies Limited;

Initiate a Risk Based Approach where appropriate organization's controls must be developed according to the degree of risk associated with the processing activities.

Complies with data protection law and follow good practice.

Protects the rights of staff, customers and partners.

Is open about how it stores and processes individual's data.

Protects itself from the risks of a data breach.

Data Protection Law

The General Data Protection Regulation (GDPR) which is designed to enable individuals to better control their personal data. It is hoped that these modernized and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by reducing regulation and benefiting from reinforced consumer trust.

The Data Protection Directive: The police and criminal justice sectors will ensure that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action. At the same time more harmonized laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe.

The General Data Protection Regulation (GDPR) describes how organizations-including Screen Technologies Limited must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or other materials.

To comply with the law, personal information must be collected and used fairy, stored safely and not disclosed unlawfully.

The General Data Privacy Rules (GDPR) is underpinned by eight important principles. These say that personal data must;

Be processed fairly and lawfully

Be obtained only for specific, lawful purposes.

Be adequate, relevant and not excessive.

Be accurate and kept up to date.

Not be held for any longer than necessary.

Processed in accordance with rights of data subjects.

Be protected in appropriate ways.

Requiring the consent of subjects for data processing

Anonymizing collected data to protect privacy

Providing data breach notifications

Safely handling the transfer of data across borders

Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

Not be transferred outside the European Economic area (EEA), unless that country or territory also ensures an adequate level of protection.

What is “Personal Data”?

“Personal data” is defined in both the Directive and the GDPR as any information relating to any person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

People, Risks and Responsibilities

Policy Scope

This policy applies to;

The head office of Screen Technologies Limited.

All branches of Screen Technologies Limited.

All staff and volunteers of screen Technologies Limited.

All contractors, suppliers and other people working on behalf of Screen Technologies Limited.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include;

Names of individuals.

Postal addresses.

Email addresses.

Telephone numbers.

....plus any other information relating to individuals.

Data Protection Risks

This policy helps to protect Screen Technologies Limited from some very real data security risks, including;

Breaches of Confidentiality.

For instance, information being given out inappropriately.

Failing to Offer Choice.

For instance, all individuals should be free to choose how the company uses data relating to them.

Reputational Damage.

For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Screen Technologies Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility;

The board of directors is ultimately responsible for ensuring that Screen Technologies Limited meets its legal obligations.

The **Data Protection Officer**, is responsible for;

Keeping the board updated about data protection responsibilities, risks and issues.

Reviewing all data protection procedure and related policies in line with an agreed schedule.

Arranging data protection training and advice for the people covered by this policy.

Handling data protection questions from staff and anyone else covered by this policy.

Dealing with requests from individuals to see the data Screen Technologies Limited holds about them also called subject access requests.

Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.

Monitoring compliance including managing internal data protection activities, training data processing staff, and conducting internal audits.

Advising with regard to data protection impact assessments when required under Article 33 - GDPR.

Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.

Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

The **IT Manager**, is responsible for;

Ensuring all systems, services and equipment used for soaring data meet acceptable security standards.

Performing regular checks and scans to ensure security hardware and software is functioning properly.

Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The **Marketing Manager**, is responsible for;

Approving any data protection statements attached to communications such as emails and letters.

Addressing any data protection queries from journalists or media outlets like news papers.

Where necessary, working with other staff to ensure marketing initiative abide by data protection principles.

General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request if from their line managers.

Screen Technologies Limited will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below;

In particular, strong passwords must be used and they should never be shared.

Personal data should not be disclosed to unauthorized people, either within the company or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed off.

Employee's shoals request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Customer right over Data

The customers rights over their data include:

The identity and the contact details of the controller and Data Protection Officer (DPO)

The purposes of the processing for which the personal data are intended

The legal basis of the processing.

Where applicable the legitimate interests pursued by the controller or by a third party;

Where applicable, the recipients or categories of recipients of the personal data;

Where applicable, that the controller intends to transfer personal data internationally

The period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;

The existence of the right to access, rectify or erase the personal data;

The right to data portability;

The right to withdraw consent at any time;

and the right to lodge a complaint to a supervisory authority;

Data Storage

These guidelines describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason;

When not required, the paper or files should be kept in a locked drawer of filling cabinet.

Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.

Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts;

Data should be protected by strong passwords that are changed regularly and never shared between employees.

If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

Data should only be stored on designated drives and servers, and should only be updated to an approved cloud computing services.

Servers containing personal data should be sited in secure location, away from general office space.

Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

All servers and computers containing data should be protected by approved security software and firewall.

There are several possibilities to protect data, Data should be encrypted before storage in a either a tokenized, pseudonymizing and complete encryption format.

Data Use

Personal data is of no value to Screen Technologies Limited unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

When working with personal data, employees should ensure the screen of their computers are always locked when left unattended.

Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

Data must be encrypted before transferred electronically. The IT manager can explain how to send data an authorized external contact.

Personal data should never be transferred outside of the European economic area.

Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

The more important it is that the personal data is accurate, the greater the effort screen technologies limited should put into ensuring it accuracy.

It is the responsibility of every employee who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Staff should every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

Screen Technologies Limited will make it easy for data subject to update the information Screen Technologies Limited holds about them. For instance, via the company website.

Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the data base.

It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject Access Requests

Consent is a basis for legal processing (along with legitimate interests, necessary execution of a contract and others). Consent means "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;"

All individuals who are the subject of personal data held by Screen Technologies Limited are entitled to:

To provide written consent/or accept to Ask what information the company holds about then and why.

Ask how to get access to it.

Be informed how to keep it up to date.

Be informed how the company is meeting its data protection obligations.

If the individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at [email address]. The data controller can supply a standard request form, although individual do not have to use this.

Individuals will be charged $25 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulations allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, screen technologies limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Data breach protocols

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification referred to in paragraph 1 shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

A description of what the company has done to stop and address the breach and any efforts the company has taken to prevent adverse effects from the breach.

Providing information

Screen Technologies Limited aims to ensure that individuals are aware that their data is being processed, and that they understand.

How the data is being used

How to exercise their rights

To these ends, the company has privacy statement, setting out how data relating to individuals is used by the company.

[*This is available on request. A version of this statement is also available on the company’s website. www.screenaml.com*]