Esland North Limited - HR

GD0003 - Data Protection Policy

Suite 1 & 5, Riverside Business Centre, Foundry Lane, Belper, DE56 0RN

v1 Last Reviewed: Miriam Berramou (Head of People Services) Tue Apr 02 2024
Next Review: Mark Calderbank - Chief Finance Officer Tue Apr 01 2025

Introduction

The UK General Data Protection Regulation (GDPR) came in to force on the 25th May 2018. It runs in parallel with the UK Data Protection Act 2018 (DPA).
The GDPR and DPA lays down rules relating to the protection of individuals (data subjects) and protects their fundamental right to the protection of their personal data and how their personal data is used by Esland.
Esland, and its entire workforce, are subject to, and must comply with, the GDPR and all associated policies. Esland's workforce includes all of the following:

- Employees
- Volunteers
- Directors
- Trustees
- Consultants
- Contractors

Data Protection Officer (DPO)

Esland has appointed a Data Protection Officer, Mark Calderbank.

- There is a legal requirement to inform the Information Commissioners Office of the details of the DPO.
- In the performance of their tasks, Esland DPO must have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.
- Esland DPO must be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The duties of a DPO are:

- Informing and advising Esland, and its workforce, of their obligations relating to the regulations
- Monitoring compliance with this regulation, and with Esland policies relating to the protection of personal data, including:
- The assignment of responsibilities
- Awareness- raising
- Training of staff involved in processing operations and
- Any related audit
- Providing advice where requested
- Ensuring Esland complies where requested
- Ensuring Esland complies with the requirement of privacy by design by promoting the use of privacy impact assessments
- Co-operating with the Information Commissioners' Office and to act as the contact point on issues relating to processing; including the prior consultation with the Commissioner's Office. In all cases where a data protection impact assessment indicates that the processing would result in a higher risk, and to consult, where appropriate on any other matter.

Training

GDPR training is compulsory for the whole of Esland's workforce as defined in 1.3 and shall provide an overview of the requirements of GDPR and must set out the responsibilities of Esland's workforce in relation to the regulation.
Access to Esland's databases and systems is not permitted unless GDPR training has been completed. Administrators for these systems are responsible for ensuring that all necessary training has been completed.
GDPR training is completed during induction and refreshed when there is an update to regulation or as required by Esland.
GDPR training will be monitored by L&D.

Definitions

Personal data means any information relating to an identifiable natural person (data subject)
The GDPR specifies that special categories of personal data is defined as data about a data subject's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic and biometric data
- health
- sexual life or sexual orientation

A data subject is anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, culture or social identity of that natural person.
Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structure, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In short, doing anything with personal data is processing.
A data controller is the person, public authority, agency or other body which decides what the purpose is for processing personal data and how it is processed. Esland is the data controller for all the personal data it processes about its workforce, members and users of its services.
A data processor means a person, public authority, agency or other body which processes personal data on behalf of a controller.
Privacy by design is an approach to projects and processes that promotes privacy and data protection compliance from the start, for example when:

- building new IT systems for storing or accessing personal data
- developing policies or strategies that have privacy implications
- embarking on personal data sharing initiatives
- using personal data for new purposes.

Privacy Impact Assessments (PIA's) are a tool used to identify and reduce the privacy risks of processing personal data and are an integral part of taking a privacy by design approach

Principles relating to processing personal data

The GDPR is based on six principles which state that personal data must be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which the personal data is being processed
- Processed in a manner that ensures appropriate security of the personal data. Including protection against unauthorised or lawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

Each principle is explained in more detail in the sections below.
The GDPR further requires that Esland must be able to demonstrate compliance with these principles. This is referred to as the accountability principle.

Accountability Principle

Esland will demonstrate that it complies with GDPR by implementing appropriate technical and organisational measures. This includes:

- GDPR policies and procedures
- Mandatory staff training
- Audits, of processing activities
- Maintenance of relevant documentation on processing activities
- Implementing measures that meet the principles of data protection by design and data protection by default

Esland's documentation on processing activities will be via its processing activity register (also known as a data asset register). The processing activity register shall contain the following information:

- The name and contact details of Esland DPO
- A description of the processes in which the processing of personal data take place and the purposes of these processing activities
- The legal basis for all personal data processing activities
- A description of the categories of data subject and the categories of personal data processed by each function within Esland
- The categories of recipients to whom the personal data has been or will be disclosed by each function within Esland
- Where applicable, transfers of personal data to another country or international organisation
- How long each category of personal data shall be retained
- A general description of the technical and organisational security measures taken to protect and safeguard the personal data

Any new project or change of process that results in a change to the processing of personal data or a new personal data processing activity must be documented in Esland processing activity register.

Any new project or change of process that involves processing personal data must comply with privacy by design requirements and undergo a privacy impact assessment.

Any activity involving personal data that is not documented in Esland's Processing Activity Register could be deemed illegal.

The lawfulness of processing personal data

The first principle states that personal data must be processed lawfully, fairly and transparently. The lawfulness of processing all personal data must be decided by Esland DPO and be documented in Esland processing activity register.

To be lawful, at least one of the following must apply:

- The data subject has given their **consent** to the processing of his or her personal data for one or more specific purpose
- The processing of the data is necessary for the performance of a **contract** to which the data subject is party to, or necessary in order to enter into such a contract
- The processing of the data is necessary for compliance with a **legal obligation** to which Esland is subject to
- The processing is necessary to protect the **vital interests** of a data subject
- The processing is necessary for the purposes of the **legitimate interests** pursued by Esland except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, where the data subject is a child.

If personal data is to be processed for a purpose different to the one for which it was collected, an assessment must be made to establish whether the new purpose is lawful. The assessment must be referred to the DPO and the decision documented in Esland processing activity register.

The lawfulness of processing special categories of personal data

Additional rules apply to special categories of personal data. The lawfulness of processing any special category of personal data must be decided by Esland's DPO and be documented in the Esland processing activity register.

In relation to the processing of any special category of personal data, to be lawful at least one legal basis from section 7.2 **and** one of the following must apply:

- The data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller of the data subject in the fields of employment, social security, and social protection in so far as it is authorised by union or member state law or a collective agreement pursuant to member state law providing for appropriate safeguards for the fundamental rights and interests of the data subject
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out during its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of UK law or pursuant to contract with a health professional
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Conditions for consent

The GDPR sets a high standard for consent, and it must offer individuals real choice and control. Genuine consent puts individuals in charge, builds trust and engagement and enhances Esland's reputation.
Where the legal basis for processing personal data is based on consent, you must be able to evidence that the data subject has consented to processing of his or her personal data.
Where the legal basis for processing personal data is based on consent, it must be unambiguous and involve a clear affirmative action (an opt-in). Pre-ticked opt-in boxes must not be used to capture any form of consent.
Where the legal basis for processing personal data is based on consent, consent should not be a pre-condition of signing up to a service and the data subject must be able to withdraw his or her consent at any time.
Withdrawing consent must be as easy to withdraw as it was to give.
Requests for consent to process personal data must be presented in a way that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this regulation shall not be binding.
Where the legal basis for processing personal data is based on consent, that consent must meet the standard of consent set out by the GDPR. Consent obtained prior to 25 May 2018 must meet the GDPR standard. Where this is not the case, new or fresh consent must have been obtained.

Specified, explicit and legitimate purpose

The second principle states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose. Collecting personal data 'just in case' is not an adequate purpose.
All of Esland's workforce must ensure that there is clarity about the purpose for which personal data is collected and used.
All specified, explicit, and legitimate purposes must be approved by Esland's DPO and be documented in the Esland processing activity register.

Adequate, relevant and limited

The third principle states that personal data must be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed.

All of Esland's workforce must ensure that there is clarity about what information is required to meet the specific, explicit and legitimate purpose for which personal data is needed. Only the information needed to meet that purpose may be collected, information not needed cannot be collected.
Collecting personal data "just in case" will be deemed to be excessive and a breach of the GDPR.

Accurate and kept up to date

The fourth principle states that personal data must be accurate and, where necessary, kept up to date.
All of Esland's workforce must ensure that they have adequate procedures in place to ensure that personal data is accurate and that all notifications of changes to the accuracy of the data are actioned without delay.

Retention of personal data

The fifth principle states that personal data must be kept for no longer than is necessary for the purposes for which the personal data is being processed.
The rules setting out how long records containing personal data may be kept are contained in Esland Records Retention Schedule, which describes each record, sets out the period for which they are to be retained and provides some examples. Where relevant, the schedule identifies the reason (legislative, regulatory and / or operational) on which retention is based and how the records are managed.
All of Esland workforce are responsible for ensuring that all records, and the personal data contained in them, are managed in accordance with Esland's Records Retention Schedule.
Disposing of personal data sooner than is set out in Esland's records retention schedule is likely to be a breach of the GDPR.
Keeping personal data for longer than is set out in Esland's records retention schedule is likely to beach of the GDPR.

Security of personal data

The sixth principle states that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Esland shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
Esland will take appropriate technical and organisational measures to protect all personal data held on and within its IT infrastructure. Esland Information Systems Controller is responsible for maintaining the security of Esland's IT infrastructure and for ensuring that regular tests are carried out to ensure that security is maintained.
All of Esland workforce is responsible and accountable for assessing the risks that are presented by processing the personal data for which they are responsible and to put in place appropriate technical and organisational measures to prevent:

- accidental or unlawful destruction, loss or alteration of personal data
- unauthorised disclosure of, or access to, personal data

All mobile phones, smart devices and tablets which have access to Esland's IT network and e-mail system must be password or PIN protected. This includes any personal devices that are being used to access Esland's IT systems and which may hold special categories of personal data in the form of e-mails and attachments which belong to Esland. The password must be unique to the user and not the default password which is assigned to the phone.
Appropriate technical and organisational measures taken by Esland to safeguard personal data are:

- mandatory GDPR training for all Esland workforce
- password protecting electronic files that contain confidential and special categories of personal data
- sending documents containing confidential or special categories of data via password protected e-mail attachments or via secure email and paper documents by special or recorded delivery
- keeping confidential and all forms of personal data in locked cabinets or locked drawers

- not leaving all forms of personal data unattended on computer screens, desks, filling cabinets or on top of printers uncollected
- locked computer screens at all times when left unattended
- a DPO approved contract or data processing agreement with third parties outside of Esland who process personal data on our behalf
- never recording the front details of a credit card and the three digit security number when processing financial data
- securely disposing of paper files and records which contain confidential and all forms of personal data by shredding them and never throwing them in the waste paper bin intact

Files containing confidential and special categories of data must be stored on Esland network; with access only available to authorised members of staff. This data should be password protected and only be copied to laptops or other mobile storage devices on a temporary basis for a specific purpose, then copied back to the network and deleted from the laptop or other device once it is no longer required.

Passwords

Passwords are essential to keep data secure from unauthorised access and accidental misuse. Passwords also prevent malicious destruction of data and protects individuals from accidentally erasing data through error.

All passwords should be reasonably complex and difficult for unauthorised people to guess. Staff should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, punctuation marks and other special characters. These requirements will be enforced with software when possible.

Passwords must never be shared with anyone else within Esland, including co-workers, managers, administrative assistants or IT staff.

Passwords must never be shared with outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

Passwords should never be written down.

Transporting or Sending Personal Data

Before any personal data is removed from Esland's office, staff must establish whether it contains special categories of data.

Whenever any personal data leaves any Esland premises, whether it is by post, carried by hand or sent by e-mail, staff must assess the risks to the data subject and to Esland if the data is lost or stolen. As part of this process, staff must assess:

- the likely impact on the data subject if the data is lost or stolen
- the likely consequences for Esland if the data is lost or stolen
- what measures are necessary to ensure that every reasonable precaution has been taken to prevent the data from being lost or stolen.

Where necessary, assessments on the risks of removing special categories of data, (including the measures taken to ensure the safety of any special categories of data), must be kept on record and produced as evidence in the event of a breach.

To ensure that every reasonable precaution has been taken to prevent data from being lost or stolen whilst in transit, the following measures should be taken. Please note this list is not exhaustive.

- checking the envelope is correctly addressed
- sending the document(s) by Royal Mail's special delivery service or via recorded delivery
- clearly marking the envelope 'private and confidential'
- ensuring that the documents are packaged securely
- when transporting documents by hand, keeping them with you at all times and not leaving them unattended
- when sending sensitive personal data or confidential data electronically, ensure that the content is either sent as an attached password protected word document or the data is anonymised.

When sending confidential and special categories of data both inside and outside of the organisation electronically, i.e. via e-mail, ensure attachments are password protected. Confidential and sensitive personal data should not be sent in the body of an email but should be sent as a password protected attachment.

In the event of a breach, where the data subject has provided explicit written consent for their sensitive personal data to be sent outside of Esland's, the staff member responsible must be able to provide evidence that every possible measure was taken to ensure the safety of the data

Mailing lists that contain large numbers of names and addresses must be password protected before being sent as an email attachment.

If there is a need to send confidential and special categories of data physically rather than electronically, it must be transported by a trusted source, either with a colleague in a locked bag, via a courier or by special or recorded delivery

Personal data being transported on a memory stick; it must be password protected and ideally encrypted. The recipient should also be contacted to confirm the data has reached its destination and a record kept of what data has been provided and to whom.

When sending emails, particularly those which contain personal data, the email must only be sent to those members of staff who need to be kept informed.

When using portable storage media such as laptops, memory sticks etc. to store sensitive personal data the device must be encrypted

Privacy by design and privacy impact assessments (PIAs)

Privacy by design is an approach to ensure that privacy and GDPR compliance is built into the initial design stages of:

- any new IT system that includes storing or accessing personal data
- any new policy or strategy that has privacy implications
- any change in the processing of personal data, such as a new employee wellbeing program or CCTV camera installation

All projects that involve the processing of personal data or change the way in which existing personal data is processed, must undertake a PIA to ensure privacy by design.

PIAs are a tool to identify and reduce the privacy risks of personal data processing and can reduce the risks of harm to individuals through the misuse of their personal information. It can also help in the design of more efficient and effective processes for handling personal data.

All PIAs must use Esland's PIA template.

Data controllers and data processors

Data Controllers

A data controller is any organisation or person that decides the purpose for processing personal data and how it is processed. As it decides what the purpose is for processing personal data about the people we support, its workforce and its members, Esland is a data controller.

As a data controller, Esland is, responsible for being able to demonstrate that its processing of personal data is performed in accordance with the GDPR.

As a data controller, Esland is responsible for ensuring privacy by design is built into all new processing activities, or changes to existing processing activities, that involve personal data.

Data Processors

A data processor is any organisation or person that processes personal data on behalf of Esland. Anyone that Esland shares personal data with, in order that they do something with it on our behalf, is a data processor.

Where processing is carried out on behalf of Esland, we must use only processors providing sufficient guarantees that they have appropriate technical and organisational measures to ensure that processing meets the requirements of GDPR, and they are able to ensure the protection of the rights of the data subjects whose data they are processing. These guarantees must be documented and up dated on a regular basis.

As a data controller, Esland must clearly set out, in the form of a contract or data processing agreement that is binding on the processor with specific regard to the processing of personal data on Esland's behalf:

- the purpose of processing
- the intended duration of processing
- a description of the personal data to be processed on our behalf

- the categories of data subjects
- the obligations and rights of the controller.

All contracts and data processing agreements with processors must be reviewed by Esland DPO to ensure that it contains sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this regulation.

The DPO shall keep and maintain a register of data processors. This register shall include who the data processor is, the purpose for which they are processing the data, a description of the technical and organisational measures and a copy of the contract or data processing agreement.

Where Esland's DPO deems that a processor determines the purpose and means of processing personal data covered by a data processing agreement, that processor shall be a controller in respect of that processing.

No processor may engage another processor without prior specific or general written authorisation of Esland. In the case of general written authorisation, the processor shall inform Esland of any intended changes concerning the addition or replacement of other processors, thereby giving Esland the opportunity to object to such changes.

Data Subject Rights

Transparency

All data subjects must be provided with information about the processing of their personal data. This information must be concise, transparent, intelligible and easily accessible, using clear and plain language. This information must be communicated at the time that the data is collected or, no later than one month after the data is collected.

All of the following data subjects whose personal data we are processing at the time that GDPR comes into force, must be provided with information about the processing of their personal data:

- Anyone Esland currently provides a service to.
- All current members of Esland's Workforce as defined in 1.3.

17.1.3 Whenever personal data is collected directly from the data subject (or their representative), the data subject must be provided with the following:

- information clearly identifying Esland as the data controller
- an explanation of the purpose(s) for which their personal data will be processed
- the legal basis for which the personal data will be processed
- who the personal data is likely to be shared with.
- how long the personal data will be stored
- Where applicable, the fact that the controller intends to transfer personal data to another or international organisation along with the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available
- an explanation of their right to request access to their personal data
- an explanation of their right to request rectification or erasure of their personal data, to restrict the processing of their personal data subject, to object to processing their personal data and their right to data portability
- where the legal basis for processing their personal data is based on consent, an explanation of their right to withdraw consent at any time
- an explanation of their right to lodge a complaint with a supervisory authority
- an explanation of their right to know the source of the personal data originated, and if applicable, whether it came from publicly accessible sources
- an explanation of their right to know of the existence, and information about, automated decision-making, including profiling

Whenever personal data about a data subject is obtained, but NOT from the data subject, in addition to the above, the data subject must be told, and the categories of personal data explained.

It is the responsibility of staff to ensure that the information set out in 17.1.3 is communicated at the time that the data is collected or, no later than one month after the data is collected.

The information in must be provided, in the first instance, in writing. However, if requested by the data subject, the information may be provided orally.

If the data subject is a child, this information must be communicated in a way that the child will understand.

A record must be kept of all instances of when a data subject is provided with the above information.

Right of access

All data subjects have the right to obtain from Esland confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and the following information:

- the purpose of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in other countries or international organisations
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- the right to lodge a complaint with a supervisory authority
- where the personal data is not collected from the data subject, any available information as to their source
- the existence of automated decision-making, including profiling, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

All requests from data subjects to access their personal data MUST be forwarded to Esland's DPO immediately and not more than 24 hours after receipt of the request. All requests must be completed within 30 days.

Deciding what information a data subject may, and may not, be given access to can be complicated and involve the application of exemptions. Therefore, ALL requests for access to personal data MUST be dealt with by Esland's DPO.

Failure to notify Esland's DPO of a request to access personal data may result in a failure to up-hold the rights of the data subject and a breach of the GDPR.

Failure to notify Esland's DPO of a request to access personal data may result in a data subject being provided with personal data that they are not entitled to. This may result in a failure to up-hold their rights and a breach of the GDPR.

Right of rectification or erasure (right to be forgotten)

Data subjects have the right to request Esland, without undue delay, to carry out the rectification of inaccurate personal data concerning him or her and the right to the erasure of personal data concerning him or her. This is also referred to as the 'right to be forgotten'.

Deciding whether personal data may be rectified or erased can be complicated and involve the application of exemptions. Therefore, ALL requests for personal data to be rectified or erased MUST be dealt with by Esland's DPO and must therefore be forwarded immediately and not more than 24 hours after receipt of the request.

A failure to inform Esland's DPO of a request from a data subject exercising their right of rectification or erasure of personal data concerning him or her could result in a breach of GDPR and may lead to action being taken against Esland. Such a failure may also result in disciplinary action.

Right to restrict processing

Data subjects have the right to request that Esland restrict the processing of their personal data.

All requests from data subjects exercising their right to request a restriction in the processing of their personal data MUST be forwarded to Esland's DPO immediately and not more than 24 hours after receipt of the request.

Deciding what restrictions must be applied can be complicated and involve the application of exemptions. Therefore, ALL requests for the processing of personal data to be restricted are dealt with by Esland's DPO.

A failure to inform Esland's DPO of a request from a data subject exercising their right to obtain a restriction in the processing of their personal data could result in a breach of GDPR and may lead to action being taken against Esland. Such a failure may also result in disciplinary action.

Right to data portability

Data subjects have the right to receive from Esland's personal data concerning him or her in a structured, commonly used and machine-readable format and to have that data transmitted directly from Esland to another controller, where technically feasible, without hindrance.

All requests from data subjects exercising their right to data portability MUST be forwarded to Esland's DPO immediately and not more than 24 hours after receipt of the request.

Deciding what restrictions must be applied can be complicated and involve the application of exemptions. Therefore, ALL requests from data subjects exercising their right to data portability are dealt with by Esland DPO.

A failure to inform the DPO of a request from a data subject exercising their right to data portability could result in a breach of GDPR and may lead to action being taken against Esland. Such a failure may also result in disciplinary action.

Right to object and automated decision making

Data subjects have the right to object to Esland processing their personal data and to object to automated decisions being made about them using their personal data.

Decisions relating to the right to object to Esland's processing their personal data and to object to automated decisions can be complicated and involve the application of exemptions. Therefore, ALL objections to Esland processing personal data and automated decision-making MUST be dealt with by Esland's DPO and must therefore be forwarded immediately and not more than 24 hours after receipt of the request.

A failure to inform Esland DPO of a data subject exercising their right to object to Esland processing their personal data and to automated decision making could result in a breach of GDPR and may lead to action being taken against Esland. Such a failure may also result in disciplinary action.

Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her.

All automated decision-making processes must be subject to a Privacy Impact Assessment and be approved by the DPO.

Children's Personal Data

Children must have protection should Esland ever collect and processes their personal data (although this is unlikely to ever occur). This is because they may be less aware of the risks involved. When this policy refers to a child, it means anyone under the age of 16. When this policy refers to someone with parental responsibility for a child it means someone who, according to the law in the child's country of residence, has the legal rights and responsibilities for a child that are normally afforded parents. This will not always be a child's 'natural parents' and parental responsibility can be held by more than one person.

A lawful basis for processing a child's personal data is needed and must be documented. The lawfulness of processing all personal data will be decided by Esland DPO and be documented in Esland's processing activity register.

Consent for all children aged 16 and under MUST be obtained from the person or persons who have parental responsibility for the child.

Any decision to allow an adult with parental responsibility to exercise a child's rights under GDPR must be taken by Esland DPO.

Reasonable efforts must be made to verify that any person with parental responsibility that is giving consent to process a child's personal data, does hold parental responsibility for the child.

Compliance with the GDPR principles, and in particular fairness, is central to all of Esland processing of children's personal data.

Processing personal data relating to criminal convictions and offences

Processing personal data relating to criminal convictions and offences, or related security measures may only be carried out under the control of official authority or when the processing is authorised by UK law.

Sharing personal data as part of a Police investigation

Occasionally, Esland may be asked to share personal data as part of a Police Investigation. This includes access to images captured by CCTV Cameras.

Any request by the Police for Esland to share personal data MUST be made in writing and include an explanation as to why the data is needed. All such requests MUST be passed to Esland's DPO. No information should be provided to the Police unless the request has been assessed by Esland DPO and a legal basis for sharing is established.

Direct marketing and the privacy and electronic communications regulations (PECR)

Direct marketing

Direct marketing is defined as: the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. All direct communications, as well as the promotion of aims, objectives and ideals are covered by the definition of direct marketing.

Legitimate service-based communications to our service users and those making an enquiry is not covered by the definition of direct marketing and is permitted under GDPR, as long as the communication is compatible with the purpose for which the personal data is being processed.

All activity marketing Esland, its services, its aims and activities must be approved by Esland marketing manager.

Esland marketing manager is responsible for ensuring that all data provided to them for the purpose of sending marketing communications, complies with the GDPR, privacy and electronic communications regulations (PECR).

Esland's marketing manager is responsible for ensuring that all marketing complies with all relevant marketing standards and codes of practice.

The only valid legal basis for processing personal data for the purpose of marketing is consent or legitimate.

Where legitimate interests is being relied upon as the legal basis for processing personal data for the purpose of marketing, a legitimate interest test must be undertaken to evidence that the legitimate interests of Esland to carry out the marketing have been balanced against the interests of the individual(s) concerned and that the marketing is not unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. The use of legitimate interest for marketing must be approved by the DPO on a case be case bases. Esland considers consent the most appropriate basis for marketing.

Where consent is relied upon as the legal basis for processing personal data for the purpose of marketing, it must be freely given, specific and an informed indication of wishes by which the data subject signifies his or her agreement.

To enable the data subjects to give informed consent to be marketed to, they MUST be given access to Esland's privacy policy.

All consent to be marketed to must be documented along with the version the privacy policy consent was based on.

An individual must be able to withdraw consent for marketing at any time and must be told of this right prior to giving it.

Consent for marketing must be as easy to withdraw for an individual as it is for them to give.

As soon as someone objects, withdraws consent, or 'opts out' of Esland's marketing, their request must be recorded as soon as possible, and all marketing stopped within 21 days. When someone has 'opted out' of Esland's marketing, a reply may be sent confirming that they have unsubscribed, but Esland must not contact them again at a later date, even if it is to ask them to opt back in.

All consent for marketing must be recorded and kept accurate and up to date. All consent records must include:

- Date consent was given
- What has been consented to
- Confirmation that they have been provided with access to a copy of Esland's privacy policy
- Date and version number of Esland's privacy policy that they were provided with access to

If someone else does our marketing on our behalf, these rules must be followed and Esland is responsible for any failure.

Esland does not use bought-in marketing lists. No marketing may be carried out using bought-in marketing lists.

Children merit special protection when their personal data is used for marketing purposes and any lack of understanding or vulnerability must not be exploited.

Marketing by electronic means

Marketing by electronic means is regulated by the privacy and electronic communications regulations (PECR). All electronic marketing messages must conform to PECR, which restrict unsolicited marketing by phone, fax, e-mail, text or other electronic message.

Electronic mail is defined as: any text, voice, sound or image sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service.

PECR apply to unsolicited marketing messages. An unsolicited marketing message is one that has not been specifically requested. PECR do not restrict solicited marketing, i.e. a message that has actively been requested.
In order to comply with PECR, all electronic marketing must have a corresponding record confirming that the recipient has consented to receive Esland's marketing e-mails, faxes and texts.
Esland's ICT department is responsible for ensuring that all forms on Esland's website capture PECR standard consent and include the ability to opt out or withdraw consent previously given.
Any electronic marketing messages sent to children must comply with PECR.

Telephone marketing

Unsolicited live marketing calls must not be made to:

- Anyone who has told Esland that they don't want to receive our calls; or
- Any number registered with the telephone preference service or corporate telephone preference service, unless the person has specifically consented to Esland's calls – even if they are an existing customer/tenant.

When making live marketing calls, you must always say who is calling, allow your number to be displayed to the person receiving the call and provide a contact address or Freephone number if asked.
Automated calls – calls made by an automated dialling system that plays a recorded message – must not be made unless the person receiving the call has specifically consented to receive this kind of call from Esland. Any general consent for marketing or consent received covering live calls is not enough. Consent must specifically cover automated calls.
Esland does not market by fax. No faxes may be sent for marketing purposes.

Marketing by Post

Marketing by post is not covered by PECR. All marketing by post must comply with GDPR.
Unsolicited marketing by post must not be made to:

- Anyone who has told Esland that they don't wish to receive our postal marketing; or
- Anyone registered with the postal preference service – even if they are an existing customer/tenant.

Reporting GDPR breaches

A breach of GDPR can occur for a number of reasons:

- Loss or theft of data or equipment on which data was stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where data is obtained by deceiving an organisation

Where a GDPR breach results in a risk to a data subject's rights and freedoms, Esland must inform the Information Commissioner's Office without undue delay and, where feasible, not later than 72 hours after becoming aware of it.
In order to comply with the requirement set out in 22.2, all GDPR breaches must be reported to Esland DPO immediately, and no later than 12 hours after the breach has become known. The DPO will request that the reporter of the breach completes a breach reporting form so that there is a written record of what happened. This must be completed within 24 hours of initial notification and then sent back to the DPO. Following this, the DPO will notify, if appropriate, Esland's Chief Executive. This decision will be based on the severity of the situation.
If informed, it is the responsibility of the Chief Executive to decide whether to inform the Board.
Any decision to report a breach to the Information Commissioner's Office (ICO) must consider the following:

- Whether the breach represents a risk to a data subject's rights and freedoms
- The amount and nature of personal data that has been compromised
- The action being taken to limit damage or distress to those affected by the incident
- The chronology of the events leading up to the loss of control of the data
- The measures being taken to prevent repetition of the incident

If it is decided that the ICO must be notified, this must occur no later than 72 hours after the breach became known.
The DPO may decide that there is no risk to a data subject's rights and freedoms, that all appropriate actions have been taken, that the breach has been contained and there is no requirement to refer it to the ICO. If the decision is not to inform the ICO, an explanation of this decision must be documented. This record of the decision not to self-report must be kept by

the DPO and must be provided to the ICO if requested.
Where a breach occurs, the DPO must consider informing the data subjects affected along with any other organisations that may be in a position to assist in protecting the data subjects. If the data subjects, and the other organisations, must be informed, this must be done no later than 72 hours after the breach became known.
Where a breach has been referred to the ICO, the ICO may request Esland provide a detailed written report of the incident. Such a report will reflect careful consideration of all elements of the breach, including any mitigating circumstances. This will be drafted by the DPO.

Recording of telephone calls

Staff are not permitted, under any circumstances, to record any telephone calls made on behalf of, or received by, Esland This include all calls made and received on a fixed line as well as mobile telephones and all internal calls. Members of staff found to have recorded conversations may be subject to disciplinary procedures and criminal prosecution.

Confidentiality

Esland takes its obligations of maintaining the confidentiality of personal data very seriously. All staff must respect an individual's right to confidentiality.
In order that we can provide the best possible service, it may be necessary to share information with other services or managers within Esland or external organisations. However, any sharing of this type must be compatible with the principles of the GDPR, in that there must be a legal basis for the sharing that is compatible with the purpose for which the data was collected.
During the course of their work, staff may see, hear or read confidential data relating to Esland. Confidential data must not be misused or divulged to any third party. This includes the press or media. A breach of confidence is likely to be a breach of GDPR.
All members of Esland's workforce that have access to personal data are responsible for taking the necessary steps to safeguard its confidentiality.
Even when consent to disclose has been obtained, personal data must only be used in ways that safeguard the confidentiality of the data (including appropriate anonymity where possible).
Individuals who do not have a contract of employment with Esland (and are not covered by an agreement or contract) are required to sign a data processing agreement and/or non-disclosure agreement. Where a contract is placed with another organisation for services which involve sharing or disclosing personal data, the parties concerned must also sign the agreement (see Section 16.3).
When sharing personal data, an obligation of confidentiality can only be set aside if the data subject has consented, there is a statutory obligation, or, it is in the 'public interest', such as matters concerning crime, national security etc.
When setting aside a duty of confidence for the purpose of sharing, the DPO must be consulted to ensure that it complies with the GDPR.

CCTV and GDPR

The use of CCTV is covered by the GDPR. This is because CCTV captures images from which individuals can be identified. This makes CCTV images personal data.
There must be a clear basis for processing personal data captured by CCTV. Esland processes personal data captured by CCTV for the purpose of preventing and detecting crime and monitoring safety and usage at our sites. These are the only purposes that the images generated by CCTV cameras can be used for.
Access to CCTV images must be strictly controlled and only authorized staff may access the personal data captured by CCTV.
All requests to access data contained in CCTV images must be dealt with by Esland DPO. This includes all requests from external organisations or individuals, including the Police. Esland DPO is responsible for ensuring whether the request is valid and for ensuring that any data contained in CCTV images that is shared complies with the GDPR.

All new requests for the installation of CCTV cameras on any Esland site must be assessed by Esland's DPO. Esland's DPO will ensure that a Privacy Impact Assessment is carried out to certify that the request for CCTV is valid and complies with GDPR.

Data contained in CCTV images may be retained for a maximum of 90 days, unless the data has been extracted as part of a subject access request. Data being processed as part of a subject access request is subject to the retention rules relating to the purpose of the request.

There should be an annual review of all the CCTV systems to ensure that they remain GDPR compliant. If any CCTV system is no longer GDPR compliant it must be stopped or modified.

Esland has a legal duty to inform people that it is using CCTV. CCTV warning signs are the most effective and most recommended method of doing just this and must be clearly visible and legible in all locations where CCTV is in operation. Where more than one camera is being used, this will probably require more than one sign. Wherever an individual is, they must have been made aware that they are being filmed.