GDPR Policy

Last update: July 2025

SKERN

Table of Contents

Policy Purpose & Scope *3*
Definitions *4*
Monitoring & Compliance *6*
Data Protection *7*
Introduction 7
Information Covered by Data Protection Legislation 7
Skern's Commitment 8
Roles & Responsibilities 8
Other roles 8
Data Management 9
Information Management *10*
Introduction 10
Statutory Framework 11
Governance 11
Policy Dissemination & Enforcement 12
Data Protection by Design 12
Protection of Personal Data 12
Storage of Information at Skern 12
Security of Information 13
Retention and Disposal 13
Related Policies *13*
Appendix One - Subject Access Request Flowchart *14*
Appendix 2 - Subject Access Request Form *15*
Appendix 3 - Template Response to SAR Applicant *16*
Appendix 4 - Data Protection Impact Assessment Process (DPIA) *17*

SKERN

Policy Purpose & Scope

To ensure that all electronic data is processed in accordance with the various standards and bodies regulations. To ensure all personal confidential data regarding all parties maintains its confidentiality, integrity, and availability.

By ensuring all parties personal data is managed effectively, to this end it is designed to make sure information retains its confidentiality, integrity, availability, and accountability by being managed in line with current and pending legislation throughout the organisation from the senior leadership team down.

The aim of this policy is to maintain the security and confidentiality of information, information systems, applications and networks owned or held by Skern.

The objectives of the policy are that Skern maintains the security and confidentiality of all personal data as follows:

- Confidentiality – information is not made available or disclosed to unauthorised individuals, users, or processes.
- Integrity – safeguarding the accuracy and completeness of information management.
- Availability – accessibility and usability upon demand by an authorised user.

The purpose of this policy is to outline:

- How Skern will ensure compliance with the UK GDPR and Data Protection Act 2018 (DPA 18).
- Explain the roles and responsibilities relevant to internal compliance.
- How compliance with this policy will be monitored.

This policy also outlines the Skern's approach to information management and covers:

- Roles and responsibilities.
- Managing risks to information.
- Protection of personal data.
- Storage, retention, and disposal of information.

This policy applies to all employees (including Ultimate Adventure Centre Ltd, Skern Lodge Ltd (Trading as Skern Adventure), including Skern Skills) , and especially in relation to the processing of personal data carried out by all parties, including processing carried out by employees, agency workers, external stakeholders, contractors, and processors. This policy is set out in two sections, the first one incorporates all aspects of data protection and the second covers information management within Skern.

Definitions

Employee:	An individual who works part-time or full-time for Skern Lodge ltd or Ultimate Adventure Centre Ltd under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
Third Party:	An external organisation with which IL conducts business and is also authorised to, under the direct authority of Skern, process the personal data of Skern contacts.
Personal Data:	Any information, including opinions and intentions which relates to an identified or Identifiable Natural Person.
Data Subject:	The identified or Identifiable Natural Person to which the data refers.
Contact:	Any past, current, or prospective Skern customer.
Identifiable Natural Person:	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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identification of that natural person.
Data Controller:	A natural or legal person, ICO, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Skern Lodge Ltd, Ultimate Adventure Ltd Known as 'Skern'	Skern establishment, including subsidiaries and joint ventures over which Skern exercise management control.
Process, Processed, Processing:	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making

	available, alignment or combination, restriction, erasure or destruction.
Data Protection:	The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.
Information Commission Officer (ICO):	An independent public authority responsible for monitoring the application of the relevant data protection regulation. Their role is to uphold information rights in the public interest.
Data Processors:	A natural or legal person, ICO, agency or other body which processes personal data on behalf of a Data Controller.
Consent:	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.
Special Categories of Data:	Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Country:	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.
Profiling:	Any form of automated processing of personal data where personal data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Binding Corporate Rules:	The personal data protection policies used for the transfer of personal data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Personal Data Breach:	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

	disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Encryption:	The process of converting information or data into code, to prevent unauthorised access.
Pseudonymisation:	Data amended in such a way that no individuals can be identified from the data, whether directly or indirectly, without a “key” that allows the data to be re-identified.
Anonymisation:	Data amended in such a way that no individuals can be identified from the data, whether directly or indirectly, by any means or by any person.

Monitoring & Compliance

To confirm that an adequate level of compliance that is being achieved by all employees in relation to this policy, the Data Protection Officer (DPO) will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess compliance with policy in relation to the protection of personal data, including:

- The assignment of responsibilities.
- Raising awareness.
- Training of employees.

The effectiveness of Data Protection related operational practices, including:

- Data Subject rights.
- Personal Data transfers.
- Personal Data incident management.
- Personal Data complaints handling.
- The level of understanding of Data Protection policies and Privacy Notices.
- The currency of Data Protection policies and Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

The Data Protection Officer, in cooperation with key business stakeholders from each business area, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the Skern leadership team.

Data Protection

Introduction

This policy provides a framework for ensuring that Skern meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). The company must comply with data protection legislation guided by the six data protection principles, which are summarised below. The principals require that personal data is:

- Processed fairly, lawfully and in a transparent manner.
- Used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, up to date.
- Not kept for longer than necessary.
- Kept safe and secure.

In addition, the accountability principle requires the company to be able to evidence its compliance with the above six principles and make sure that it does not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet these obligations, the company must put in place appropriate and effective measures to make sure we comply with data protection law.

Information Covered by Data Protection Legislation

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.
Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric ID data
- Health data
- Sexual life and/or sexual orientation
- Criminal data (convictions and offences)

Skern's Commitment

Skern is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about employees, guests or those who work or interact with us.

A privacy notice is published on the website. The notice is tracked and updated as necessary. There is also an employee privacy notice which has been made available to all employees.

All employees are required to undertake mandatory training on information governance, GDPR and security.

Personal data breach incidents are considered and have a reporting mechanism that is communicated to all employees. The incident is assessed as to whether it needs to be reported to the ICO as the Regulator of DPA. Appropriate action is taken to make data subjects aware if needed.

For information rights there is a clear process in place to handle subject access requests and other information rights requests as found in Appendix 1.

There is a procedure to assess processing of personal data perceived to be high risk. This requires a Data Protection Impact Assessment (DPIA) to be carried out (Appendix 4).

Roles & Responsibilities

Richard Thomas is the Data Protection Officer (DPO) and primarily responsible for advising on and assessing compliance with the Data Protection Act and UK GDPR and making recommendations to improve compliance.

Richard's contact details are:
Richard.thomas@skern.co.uk

Or contact one of our direct enquiry lines:
enquiries@skernadventure.co.uk
enquiries@skernskills.co.uk

Other roles

Specific roles are assigned throughout the company to manage personal data processed and the associated risks in terms of responsibilities, decision making and monitoring compliance.

Data Management

The GDPR and the Data Protection Act 2018 have seven principles to be followed by all Data Controllers, including:

1. Lawfulness, fairness, and transparency.

2. Purpose limitation.

3. Data minimisation.

4. Accuracy.

5. Storage limitation.

6. Integrity and confidentiality (security).

7. Accountability.

In addition to this, Data Subjects have rights to:

1. **Information about how their data is being processed.** Skern addresses this by ensuring Data Subjects are informed as to how their information is used.
2. **Access to their information.** Skern has a clear process in place to handle subject access requests and other information rights requests (Appendix 1).
3. **Rectification when information is wrong.** Any request for rectification will be assessed on a case-by-case basis using the precedent of Skern developing experience of the legislation, along with relevant case law.
4. **Be forgotten, when it is appropriate.** Any request to be forgotten will be assessed on a case-by-case basis using the precedent of Skern developing experience of the legislation, along with relevant case law.
5. **Restrict processing.** Data Subjects may request that Skern hold only sufficient Personal Data about them but not process it any further. Any request for restriction of processing will be assessed on a case-by-case basis using the precedent of Skern developing experience of the legislation, along with relevant case law.
6. **Data portability.** This allows Data Subjects to obtain and reuse their information across different services. Any request for portability of data will be assessed on a case-by-case basis using the precedent of Skern developing experience of the legislation, along with relevant case law.
7. **Object to processing.** This allows the Data Subject to object if they do not believe the use of their information is legitimate. Any request to object will be assessed on a case-by-case basis using the precedent of Skern developing experience of the legislation, along with relevant case law.
8. **Appropriate decision-making.** Skern is required to demonstrate that it has a lawful basis to carry out profiling and / or automated decision-making. This is undertaken by a regular organisation-wide assessment, led by the Data Protection Officer.

All requests from Data Subjects to exercise their rights must normally be responded to within one calendar month, unless there are extenuating circumstances, in which case there are some rights to extension under the legislation.

Information Management

Introduction

This section sets out our commitment to following good information management practices. Skern's approach is guided by the expectations set out by the ICO and is based on the principles outlined in the data protection section.

In writing this, Skern has considered the nature of the information it holds, the work it does and the legal requirement for confidentiality imposed on its employees.

Effective information management helps to ensure Skern has the right information at the right time to make the right decisions. Skern is committed to service excellence and information management is vital to the delivery of its services across the business in an orderly, efficient, and accountable manner.

Information is a valuable corporate asset, and the records provide evidence of what has been done and why. The aim is to balance Skern's commitment to openness and transparency with responsibilities.

Skern has a clear understanding of the information it holds, why it is held it and that information is managed in according to its sensitivity. Information is managed efficiently, made accessible when needed, protected and stored securely and disposed of safely at the right time.

Skern has the appropriate governance, organisational capacity, and technical measures in place to manage information in accordance with the expectations set out by the ICO.

By adopting this policy, Skern aims to ensure that information, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

- Help us carry out our business.
- Help us to make informed decisions.
- Protect the rights of our employees, guests, and external stakeholders.
- Track policy changes and development.
- Make sure we comply with relevant legislation.
- Provide an audit trail to meet business, audits, and legal requirements.
- Make sure we have the essential tools to search, identify, locate, and retrieve information.
- Support continuity and consistency in management and administration.
- Make sure IL are open, transparent, and responsive.
- Support relevant research and development.

This policy together with associated guidance and procedures applies to the management of all information, in both digital and physical formats, created or received by Skern. It applies to all employees, contractors, and external stakeholders who are given access to documents and information processing facilities.

Statutory Framework

This policy provides a framework for meeting Skern's information management responsibilities under relevant legislation, guidance and codes of practice including the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act 2000 (FOIA 2000)
- Code of Conduct

Governance

All staff have a responsibility to ensure Skern manages information and any associated risks appropriately and in accordance with this policy and its associated guidance and procedures.

To demonstrate Skern's commitment to data protection, and to enhance the effectiveness of its compliance efforts, Skern has established this GDPR Policy. The policy operates with independence and is managed by suitability skilled individuals granted all necessary authority. The Data Protection Officer reports to Chief Executive and both have direct access to all other team members.

The Data Protection Officer (DPO) whose duties include:

- Informing and advising Skern and its employees who carry out processing pursuant to GDPR, national law or UK based data protection provisions.
- Ensuring the alignment of this policy with GDPR, UK based data protection provisions.
- Providing guidance with regards to carrying out data protection impact assessments (DPIAs).
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs).
- Determining the need for notifications to one or more DPAs as a result of Skern's current or intended personal data processing activities.
- Making and keeping current notifications to one or more DPAs as a result of Skern's current or intended personal data processing activities.
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests.
- Informing senior managers, officers, and directors of Skern of any potential corporate, civil and criminal penalties which may be levied against IL and/or its

employees for violation of applicable Data Protection laws. Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this policy by any third party who:

- Provides personal data to Skern.
- Receives personal data from Skern.
- Has access to personal data collected or processed by Skern.

Policy Dissemination & Enforcement

The leadership team of Skern must ensure that all of its employees are responsible for the processing of personal data and are aware of and comply with the contents of this policy.

In addition, each employee will make sure all Third Parties engaged to process personal data on their behalf, i.e. their Data Processors, are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to personal data controlled by Skern.

Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

Skern must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the GDPR Policy, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the DPO and IT team. Where applicable, the IT team, as part of its IT system and application design review process, will cooperate with the DPO to assess the impact of any new technology uses on the security of personal data.

Protection of Personal Data

The Skern GDPR Policy provides a framework for ensuring that it meets its obligations under the UK GDPR and the DPA 2018. It applies to all the processing of personal data carried out by the Skern including processing carried out by joint employees, contractors, and external stakeholders.

Storage of Information at Skern

Skern stores its information in prescribed locations, appropriate to its format, content, and sensitivity. Skern ensures appropriate controls are in place to maintain the confidentiality, integrity, and availability of information.

Security of Information

Skern ensures the security of information via the implementation of a number of policies, procedures and guidance.

Retention and Disposal

Procedures outline Skern's approach to managing the retention and secure disposal of information. It provides for a consistent approach and applies to all physical and digital information, regardless of storage location.

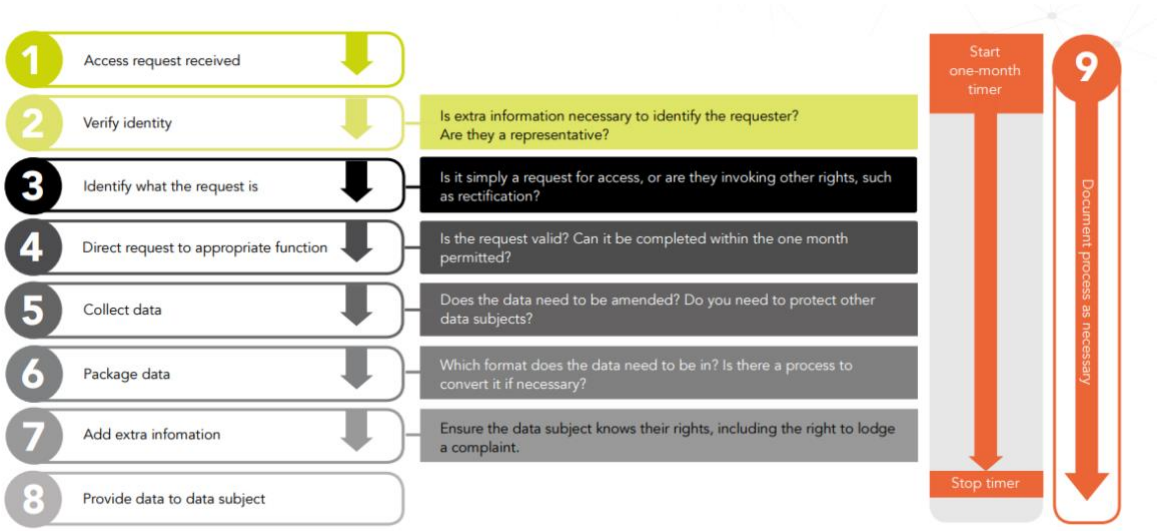
Skern's retention periods are driven by legislation or business need. If there is no legally defined retention period for corporate information, it is the responsibility of the relevant management teams to determine an appropriate retention period.

Related Policies

The following policies and information are aligned with this policy:

- Employee Handbook
- Code of Conduct

Appendix One - Subject Access Request Flowchart



1. A request can be received by anyone in the company in any format. Directors will acknowledge receipt and log on Subject Access Request Register.
2. Formal ID will only be requested if Skern does not have an ongoing relationship with the requestor.
3. Further information can be requested if required which will pause the response timeline.
4. DPO and Directors to discuss request and agree approach.
5. DPO to collect agreed data including an email swipe from IT.
6. DPO to anonymise and package data as appropriate for transmission.
7. DPO to prepare formal response to requestor.
8. DPO to send all appropriate data to requestor in the agreed format marked Private and Confidential. All correspondence will be kept on file for two years.

SKERN

Appendix 2 - Subject Access Request Form

Name:
Daytime telephone number:
Email:
Address:
Employee number:
By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the organisation that you are eligible to receive.
Required information (and any relevant dates):
By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else, including family members, unless evidence is provided of authority to act on your behalf. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost, and expenses if you are not. Please return this form to Richard.thomas@skern.co.uk Please allow 28 days for a reply.
Data subject's signature:
Date:

SKERN

Appendix 3 - Template Response to SAR Applicant

The following are example paragraphs to be used when responding to a subject access request.

Delete where not applicable.

Dear ……

Thank you for your letter dated xx\xx\xx.

* Your request is being dealt with and we will reply as soon as possible but certainly within a month as set out in the Data Protection Act 2018.

* To maintain confidentiality, the law allows us to take reasonable steps to establish and confirm your identity before we can provide any information. We would be grateful if you could provide us with proof of your identity in the form of the original version or authenticated copies from a solicitor of:

- Driving license
- Birth certificate
- Passport
- Marriage certificate
- Court order establishing legal guardianship over a child or incapacitated individual.
- Testimony or will from a solicitor establishing entitlement to a claim on the estate.

In accordance with the Data Protection Act 2018, the month we are allowed in producing you or your client's records may be suspended while we await receipt of the information requested.

* With reference to your letter of xxxx regarding access to your records, we can confirm that your request has been processed and I enclose copies of the records that you require.

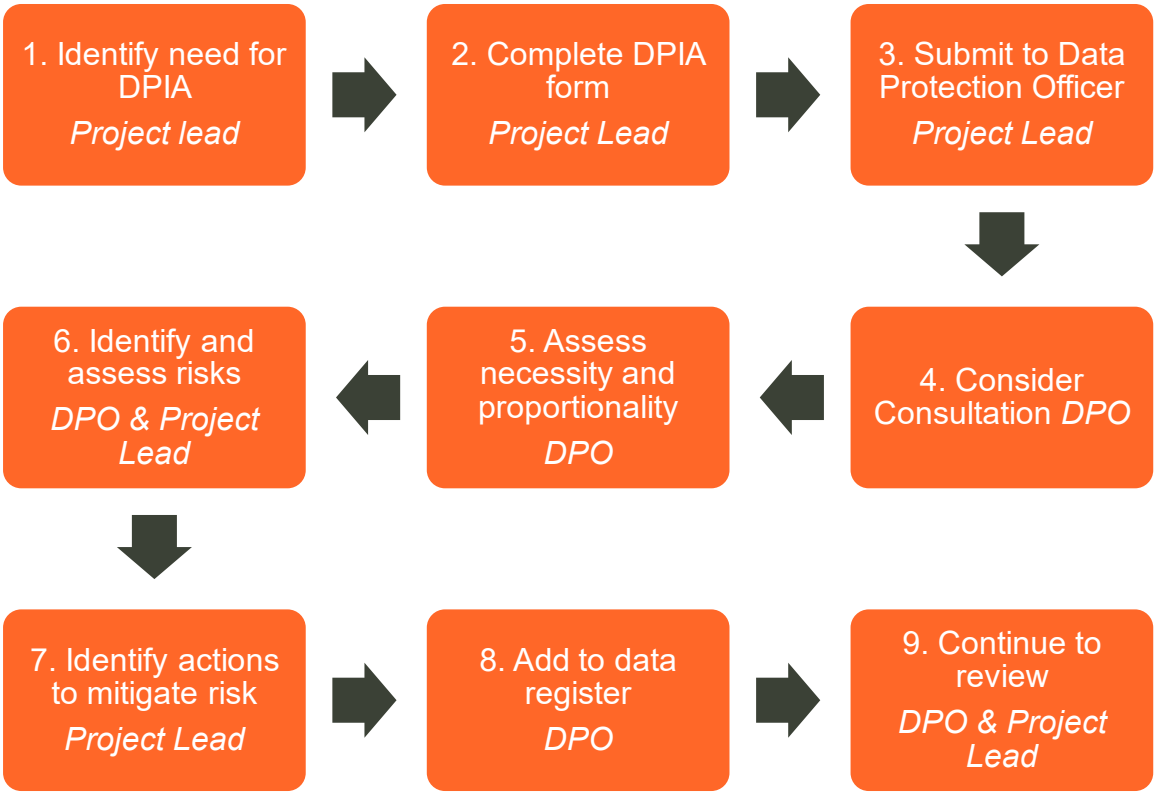
* Access to parts of the records have been declined because a) it has been considered by the company to contain certain information that should not be shared, or b) third party information has been removed.

* The records which you have requested are held by another organisation. Your application will therefore be forwarded to (organisation/3rd party). If you have any queries, please do not hesitate in contacting me at the details given above.

Yours sincerely

SKERN

Appendix 4 - Data Protection Impact Assessment Process (DPIA)



Process Notes

1. You must do a DPIA for any processing that is likely to result in a high risk to individuals. This includes some specified types of processing. You can use the screening checklist provided by the ICO to help you decide when to do a DPIA. It is also good practice to do a DPIA for any other major project which requires the processing of personal data. If in doubt, please discuss with the DPO.
2. Click on the link to access the form.
3. Forms are stored centrally.
4. Privacy notices may also need updating.
5. In relation to data processed.
6. Highlight any risks associated with the processing or storing of the data.
7. If there are no ways to mitigate high risks, the ICO must be notified.
8. Centrally held register of data held within the organisation.

SKERN