Karslakes Solicitors Limited – Privacy Standard

CONTENTS

CLAUSE

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: Karslakes Solicitors Limited

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or

our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. Introduction

This Privacy Standard is Karslakes Solicitors Limited's Data Protection Policy.

This Privacy Standard sets out how Karslakes Solicitors Limited ("we", "our", "us", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Privacy Standard applies to all Company Personnel.

3. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The DPO is responsible for overseeing this Privacy Standard. That post is held by: Michael Elford.

4. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

We will ensure that personal data is Processed lawfully, fairly and in a transparent manner.

We will only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

We will only Process Personal Data for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

5.2 Transparency (notifying data subjects)

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), when necessary we will provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data.

6. Purpose limitation

Personal Data will be collected only for specified, explicit and legitimate purposes. It will not be further Processed in any manner incompatible with those purposes.

We will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

7. Data minimisation

We will ensure that Personal Data is be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We will not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

Data Subjects will be informed of the period for which data is stored and how that period is determined.

10. Security integrity and confidentiality

10.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

10.2 Reporting a Personal Data Breach

The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

11. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

We will only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

12. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

Although Data Subjects have a right to withdraw Consent to Processing, this does not supersede our right to retain and store Personal Data for such periods that we are required to do so by any legal obligation of regulation (see clause 14).

We will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

We will put in place adequate controls to ensure and to document GDPR compliance.

12.2 Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

We will keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

12.3 Training and audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

12.4 Privacy By Design and Data Protection Impact Assessment (DPIA)

We will only collect data which is necessary and for the use for which it was initially collected. We will only keep such data for as long as we required to do so.

We will undertake Data Protection Impact Assessments when it is necessary for us to do so.

12.5 Automated Processing (including profiling) and Automated Decision-Making

We do not carry out any Automatic Processing or Automated Decision-Making.

12.6 Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing is explicitly offered to the Data Subject in an intelligible manner.

A Data Subject's objection to direct marketing will be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

12.7 Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

We will only share the Personal Data we hold with employees, agents or representatives of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We will only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and

(d) the transfer complies with any applicable cross border transfer restrictions.

13. Changes to this Privacy Standard

We reserve the right to change this Privacy Standard at any time so please check back regularly to obtain the latest copy of this Privacy Standard. We last revised this Privacy Standard on 25 May 2018.

This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Company operates.

14. Retention Periods

We operate the following file retention periods and schedule of original documents, which supersede the Data Subject's right to withdraw Consent to Processing:-

FILE RETENTION PERIODS

Category	Includes	Retention
Property Purchase & Mortgage Files	Purchase Re-Mortgage Deed of Postponement Mixed Property Purchase & Sale Deed of Easement eg: Rights of Way Deed of Covenant	**16 Years**
Property Sale & Other Property Matters	Sale of Property Planning Housing General advice	**7 Years**
Leasehold Matters	Lease Agreements Licence Agreements Variations Surrender Assignment Rent Review General Advice	**Term + 7**
Litigation	Civil Criminal Tribunals-Employment, Pensions Welfare	**7 Years**
Private Client	Non Litigation Advice-Employment Pensions, Personal Insolvency, Tax, Powers of Attorney (Non Enduring)	**7 Years**
Immigration	General Advice Tribunal Asylum	**7 Years**

Trusts, Wills & Probate	Will Drafting Probate etc Trust Matters Enduring Powers of Attorney Settlements Court of Protection	**21 Years**
Business	Compant Formation Partnership Formation Sale/Merger/ Purchase Insolvency Investment/Share Issue	**7 Years**
Divorce, Children Disputes & Ancillary Relief	Divorce Children	**3 Years after Youngest Child is 18**
Administration	Employment/Tax Records Insurance Law Soc/SRA Correspondence Diaries Manuals Electronic Records	**11 Years**
Firm Accounts	Office Account	**11 Years**
Client Accounts	Ledgers Bank Statements Stubs, Paying Slips, Receipts etc	**11 Years**

Schedule of Original Documents

1. Conveyancing Deeds
2. Abstract of Title
3. Lease/Counterpart Lease/Licence to Assign or Sub-let
4. Life Assurance/Mortgage of Life Policy
5. Power of Attorney
6. Charge Certificate
7. Land Certificate
8. Tenancy Agreement
9. Assignment of Mortgage Deed
10. Mortgage Deed/Legal Charge
11. Guarantee Certificate
12. Endowment Policy
13. NHBC Certificate
14. Leasehold Assignment
15. Assent
16. Grave Deeds
17. Deed of Covenant
18. Grant of Easement
19. Marriage and Civil Partnership Certificates
20. Birth Certificate
21. Immigration Order
22. Passport
23. Deed of Separation/Matrimonial Deeds
24. Share Certificate
25. Deed of Partnership
26. Patents and Assignments of Copyrights
27. Will/Codicil
28. Bank Pass Book
29. Retirement Policy
30. Deed of Gift/Trust
31. Investment Business/Assignment of Goodwill
32. Bonds
33. Change of Name Deeds
34. Statutory Declaration
35. Personal effects/valuable items
36. Documents of historical or archival value.