Harland & Co Solicitors GDPR Policy

Rev 1. March 2018

GDPR Policies

It is important that all relevant staff know the data collection policy in order to comply with GDPR, the EU directive regarding data security and privacy. Staff employed by this business as well as its subcontractors and suppliers must adhere to our data collection, storage and processing policy because failure to do so could render the business non compliant with GDPR. We are legally required to be GDPR compliant and we must fulfil that promise even if it sometimes seems inconvenient to do so.

Legal Basis for Collecting Personal Information

The legal basis for collecting personal information would fall under one or more of the following areas:

- Consent: If the subject provides explicit consent for the Harland & Co Solicitors to collect their data they must also be informed of their right of erasure and their right of access.

- Legally required: Data that the company is legally required to provide must be collected (for example, an employee's national insurance number that is legally required by HMRC).

- Genuine Business Interest: If Harland & Co has a genuine business interest in recording that particular item of personal data, it is perfectly legitimate for that personal data to be recorded. For example: there is a genuine business need to record the address of the customer. Such data must be collected in order that the company can fulfil its promise to provide the customer with the required standard of service.

- Vital interests: If the Harland & Co Solicitors need to pass information on to the Emergency Services or other life-saving professional in order to protect someone's life, the information will be given to that third party.

Principles of Data Collection, Storage and Processing:

Personal Data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 83(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

6. 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 ('integrity and confidentiality')

Children

It is our policy to collect data from children (persons aged under 16) only when that data is relevant to the matter about which we are providing professional services to the client (for example: family matters or custody cases). If you suspect someone may be under 16 you will need to get parental/guardian consent and proof of age before collecting any personal data form that child. We are not permitted to collect the child's personal data without the consent of their parent/guardian.

Sensitive Personal Data

It is our policy to collect sensitive personal data from customers only when the data is relevant to the professional services which we are providing to that client.

Other People's Data

We are required, in the course of carrying out our normal business, to collect data from people about other people (for example: we collect data from one adult about the rest of their immediate family if we are providing advice concerning a divorce/separation). It is our policy to collect relevant data only and to keep that data secure.

Notification

We must always notify people before we collect their data except when we collect data from someone about other people. Our Privacy Policy notifies people of their rights to access their data and our initial engagement form reiterates those rights so that people are correctly notified.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is Diane Grayson and that role includes driving remediation plans for security gaps. It is not mandatory for this company to have a DPO. The DPO is responsible for regularly reviewing and, where necessary, improving the security of personal data and is responsible for reviewing all complaints, access requests and data breaches. If a data breach is discovered, it is the DPO's responsibility to advise the individuals whose data may have been compromised and provide advice as to their best course of action in order to minimise their risk. The procedure also requires that all complaints and breaches are documented and the resulting actions taken are also documented and regularly reviewed.

Subject Access Requests

People may access their data by requesting it, providing they supply us with proof of their identity and proof of address. All requests for data erasure or provision must be forwarded to the Data Protection Officer immediately. It is a legal requirement that such requests are processed within 30 days. It is our policy that the DPO will, upon satisfactory proof of identity, process the Subject Access Request using the DPO's own ability to access the database and carry out the appropriate steps to fulfil the Subject Access Request.

An original driver's licence or original passport are accepted as proof of identity. A recent letter from the Inland Revenue or other government department or utility company is accepted as proof of address. Copies of those documents are not taken and they must be the originals (not copies). On satisfactory proof of identity and address the DPO is required to provide the person with the personal information that is kept on file – note that "personal information" does not include our records, only their own personal data which is keep on the computer database or in any other file. If the subject asks for the computerised data to be

provided in machine readable format, the Data Protection Officer will supply it in machine readable format. Data which is in physical paper files may not be provided in machine readable format.

Subject Erasure Requests

If a person asks for their data to be erased, proof of identity and address is required as for Subject Access Requests. The Data Protection Officer may then either erase the data or ensure it has been anonymised by altering all personal identifying information including but not limited to Name, Address, Post Code, phone number and any other information which could be used to identify that individual, The process is to be completed within 30 days.

The Data Protection Officer will check there are no outstanding invoices payable by the customer and that there is no genuine business requirement to retain that data, then the data will be erased or anonymised. The data backups will, in time, erase the data from backups as well because those backups will be overwritten. The Data Protection Officer will also ensure that if a backup is restored, it does not bring back into the database any Subject Erasure Requests.

Data and Profile Processing

It is our policy not to process data other than use it to communicate with the customer, ensure prompt payment and prompt service, to ensure correct provision of our services and (where the customer has opted-in) to ensure the subject is kept informed of our services. We therefore do not process customer's personal data for any other reason. It is our policy not to use data for profiling.

Data Security

It is our policy to keep personal data secure. The database is protected with appropriate passwords on the client PC and on the database itself. Therefore, it is required that these passwords are not saved in the keychain or otherwise auto-entered, they must be manually typed in every time in order to access the database. Additionally, the database is held on a server which is physically secure and out of sight of the general public and visitors.

Complaints & Data Breaches

If any member of staff discovers a data breach or receives a complaint about the processing, storage, retrieval or deletion of personal data they must contact the Data Protection Officer immediately upon becoming aware of the complaint or discovering the breach. The DPO will notify the Information Commission Officer within 72 hours.

Complaints must be made in writing with full details of the complaint, including the full names and addresses of the individuals who are affected by the incident as well as the type of data which falls within the scope of the incident. The DPO will review the complaint within 30 days and take appropriate steps to resolve the complaint. The DPO will also notify all affected individuals in a timely manner that there has been a data breach, and will make recommendations to the individuals affected as to how they can mitigate further risks (such as changing passwords etc).

Duration of Data Retention

Our policy is to retain data for as long as it is necessary for us to fulfil our legal obligations, provide our services and to protect ourselves against adverse legal representation. At present, the data retention period deemed useful to the genuine business interests of the company is as follows:

- For general matters (physical files): 6 years.
- For conveyancing matters (physical files): 15 years
- For wills etc (physical files): Forever

- Computerised records of historical transactions: Forever
- For staff: As long as the staff are employed, and for a period no more than 10 years thereafter.

Periodic reviews on the retention of data are carried out.

Suppliers and Partners

All suppliers and partners who wish to make use of personal data provided by Harland & Co Solicitors are legally required to be GDPR compliant from May 25th 2018 and must co-operate with us in ensuring the security and privacy of personal data. Suppliers and partners must not sell, lend, transfer, give or otherwise provide in any form the personal data that has been provided to them by Harland & Co Solicitors.

Data Protection Impact Assessment (DPIA)

DPIA must be carried out if the data falls within any of the following criteria:

- Evaluation or scoring, including profiling and predicting especially from aspects concerning the Data Subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements
- Automated decision-making with legal or similar significant effects
- Systematic monitoring of individuals
- Sensitive data
- Personal Data on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable Data Subjects
- Innovative use or application of technological or organisational solutions
- Data transfers across borders outside the European Union
- Data that Prevents Data Subjects from exercising a right or using a service or a contract

The Data Protection Officer will regularly assess whether or not data falls within the above criteria and ensure that a DPIA is carried out if it does.

Initial Engagement Form

The company's policy requires that customers sign acknowledgement that they have been informed of their rights under GDPR.

International

It is our policy not to transfer data to any state outside the United Kingdom.

Data Audit

The data which is collected from customers includes only relevant information such as: full name, address, phone number, email address, and any other relevant information that could be used to enhance our ability to provide services to the customer. Such additional information may include sensitive personal information providing such information is relevant.

The data which is collected from staff is by necessity detailed and could include additional data specifically required in order to satisfy the legal requirements and duty of care which the company is obliged to provide. This data may include, but is not limited to, nationality and passport number (in order to prove legality of employment), medical records, gender, next of kin and date of birth. People who are next of kin have the right to ask for their data to be erased.

Data Security & Backups

Data is not encrypted but is protected from unauthorised access by way of a conventional login and password system. Data is backed up and the backups are eventually overwritten. Servers are kept away from access by the general public and customers and only authorised personnel are provided with the login details required to access the data in the normal course of their employed duties.

External Organisations

Companies with whom personal data is shared includes other solicitors, estate agents and other professional bodies only where the third party has a genuine business need to access that data.

CCTV & Photography

It is our policy not to record images using CCTV nor to take photographs of people. Photographs of people may be given to us in the course of carrying out our professional services but those photographs will only be relevant to the issue in hand.