

## Eazi-Business Data Protection and Privacy Standard (Internal Use Only)

### Introduction

This Standard introduces our personnel and licensees to their obligations in relation to data protection and privacy. It must be read in conjunction with our privacy policies, referred to below. Those policies tell people how we deal with their personal information. This Standard in turn explains to you, our personnel, or those of our licensees or service providers, how to ensure that you and we comply with those policies.

This Standard applies to all personal data we process regardless of its format or the media on which it is stored or whether it relates to past, present or potential employees, clients, licensees, suppliers, service providers, website users or any other Individual. It is based on our operations in the UK and the laws here. If you are based outside the UK, you must also comply with all your applicable Data Protection Legislation.

This Standard is an internal confidential document and cannot be shared with third parties, clients or regulators without prior authorisation from us, the licensor. It is also subject to copyright.

Click on the links below if you want to go straight to more information on any part of this Standard:

Introduction.....	1
Who We Are .....	2
Who Must Comply with This Standard and Related Compliance .....	2
Interpretation of Certain Terms for the Purposes of this Standard .....	2
Responsibility and Consequences .....	4
ICO Guide and Further Help .....	4
Contacting the Data Privacy Manager.....	4
Personal data protection principles .....	5
Lawfulness, Fairness, Transparency (including privacy policies).....	6
Purpose Limitation .....	7
Data Minimisation .....	7
Accuracy .....	8
Storage Limitation .....	8
Security, Integrity and Confidentiality.....	8
Reporting a Personal Data Breach.....	9
International Transfer Limitation .....	9
Individuals' Rights and Requests.....	10
Accountability and Record Keeping.....	11
Training and Audits.....	11
Privacy by Design.....	11
Data Protection Impact Assessment (DPIA) .....	12
Automated processing (including profiling) and Automated Decision-Making .....	12
Direct marketing.....	12
Sharing personal data.....	13
Our Role as a Data controller or processor .....	13

## Who We Are

“We” “our” or “us” refers to the licensor company, Eazi-Business Limited. We are a limited company registered in England and Wales with registered number 08364226 and registered office at The Old School House, 65A London Rd, Oadby, Leicester LE2 5DN, UK (also using various trading names such as Eazi-Apps, Eazi-Sites, Eazi-SEO). “We” “our” or “us” also or instead refers to any group company of this company.

We are also the licensor company for many unrelated licensee companies that may use one or more of our trading names. We and all licensees in the network have no responsibility or liability for other licensees, who are all separate legal entities, nor for their personnel.

## Who Must Comply with This Standard and Related Compliance

This Standard applies to everyone when working for us, with us or on our behalf in any capacity, including employees at all levels, directors, officers, owners, licensees, agency or seconded workers, interns, agents, contractors, consultants, service providers, third-party representatives and business partners.

Our licensees must also ensure compliance within their own business with their own data protection and privacy standard with the licensee as “we”, “our” or “us” as used in this Standard. Their own standard must include obligations and prohibitions at least at the level of those in this Standard but must be adapted for their local legislation to comply with any additional or further requirements under that legislation.

You must read, understand and comply with this Standard when processing personal data on our behalf and must attend training on its requirements. This Standard sets out what we expect from you. Your compliance with this Standard is mandatory and failure to comply may result in disciplinary action or action under any contract that you have with us, in both cases that may even result in termination.

You must also comply with:

- All applicable Data Protection Legislation (which adds to this Standard since the legislation is far more comprehensive than this Standard, and which overrides this Standard if inconsistent)
- Our Privacy Policies (such as for website users or clients and for personnel / licensees) [[links](#)]
- The ICO Guide for Businesses which is very useful and detailed and is at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- Any further data protection or privacy guides or instructions provided to you
- Any of our Information Security, Cyber Security, Security or other Policies or Standards

If you have a specific responsibility such as capturing consent, reporting a personal data breach or conducting a DPIA as referenced in this Standard then you may need more detail than set out in this Standard. You should refer to the ICO Guide referred to above and contact your DPM if unsure.

## Interpretation of Certain Terms for the Purposes of this Standard

**consent:** a freely given, specific, informed and an unambiguous indication of the Individual's wishes by a statement or by a clear positive action to agree to the processing of their 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 Data Protection Legislation. We are the controller of all personal data relating to our all personnel and personal data used in our business for our own commercial purposes

**Individual:** a living, identified or identifiable individual about whom we hold personal data, irrespective of their nationality or residency

**Data Privacy Impact Assessment (DPIA):** tools and assessments (which should be recorded in writing) used to identify and reduce risks of a data processing activity

**Data Protection Manager (DPM):** the person with responsibility for data protection compliance within your company (for us as the licensor company, this means the directors). If your business requires a Data Protection Officer (DPO) to be appointed by law, then the DPM will be that DPO.

**Data Protection Legislation:** the General Data Protection Regulation ((EU) 2016/679) known as GDPR, as implemented in the UK by the Data Protection Act 2018, plus and any all other data protection and privacy legislation that is applicable to you or us in the areas in which you or we operate.

**ICO Guide:** The guide published by the Information Commissioner in the UK and updated and available on the internet (at the date of this statement it is at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>) You should look for the equivalent from your Data Protection Authority if outside the UK.

**personal data:** any information identifying an Individual or relating to an Individual 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 sensitive 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, date of birth and so on) 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. Loss or unauthorised access, disclosure, copying or acquisition of personal data are all personal data breaches.

**personnel:** all employees, workers, contractors, agency workers, consultants, licensees, directors, owners, members and anyone else working for us / you in any capacity

**privacy policies:** separate notices setting out information provided to Individuals (this may be by link to a policy on our website) when we collect information about them. These notices may take the form of general privacy policies applicable to groups of individuals (for example, employee / licensee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy notices 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 anyone external.

**sensitive data:** For convenience in this Standard, we combine and refer to as “sensitive data” terms referred to in Data Protection Legislation separately as “Special Categories” of personal data and “Criminal Convictions Data”. In this Standard, sensitive data therefore means: 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, personal data relating to criminal convictions or offences including criminal allegations and proceedings.

## Responsibility and Consequences

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.

Apart from the loss of reputation and business if there is a personal data breach, the fines and consequences can be very severe. For example, every company or person that does not comply with Data Protection Legislation from the UK or EEA can be exposed to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher.

All licensees, directors and managers are responsible for ensuring all personnel comply with this Standard and must implement appropriate processes, controls and training to ensure that compliance. The DPM is responsible for overseeing this Standard and, as applicable, developing further policies and advice.

## ICO Guide and Further Help

You should read the website of the data protection authority in your country, which generally have useful guides and information, and may be more updated more frequently than this standard. We do not recommend doing internet searches or copying other businesses because a lot of companies have out of date materials or policies and there is a lot of misinformation on the internet on this topic.

In the UK, you should go to [www.ico.org.uk](http://www.ico.org.uk) which is very informative. It includes the ICO Guide for businesses which refers to the data protection legislation in the UK, which in summary is the GDPR adapted and implemented within the UK by the Data Protection Act 2018.

You **must by law be registered with the ICO** (and pay their fee) for each business in the UK. Outside the UK, you need to check the requirements with your local data protection authority (search for this or data protection regulator or privacy authority). For example, a list of the European data protection authorities can be found (at the date of this Standard) here: [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en)

The ICO Guide is far more detailed than this Standard and should be read carefully for further detail on any matter related to data protection or privacy. It is kept updated and should be your primary source for information. In addition to the ICO Guide, the ICO has for example:

- Videos, which are useful for training <https://www.youtube.com/user/icocomms/videos>
- A helpline for SMEs (small and medium enterprises) which you can phone for any advice:
- A special section for SMEs: <https://ico.org.uk/for-organisations/business/> and a sole trader toolkit.

## Contacting the Data Privacy Manager

Please contact your DPM with any questions about the operation of this Standard or data protection legislation or if you have any concerns that this Standard is not being or has not been followed. You must always contact your DPM in the following circumstances (see separate headings for more detail):

- if you are unsure of the lawful basis which you are relying on to process personal data (including the legitimate interests used);

- if you need to rely on consent and/or need to capture Explicit consent or are thinking of doing so;
- if you need to draft Privacy Notices;
- if you are unsure about the retention period for the personal data being processed;
- if you are unsure about what security or other measures you need to implement to protect personal data;
- if there has been a personal data breach (this contact is urgent and important);
- if you are unsure on what basis to transfer personal data outside the EEA, UK or your country;
- if you need any assistance dealing with any rights invoked by an Individual;
- whenever you are engaging in a significant new, or change in, processing activity which is likely to require a DPIA or plan to use personal data for purposes other than what it was collected for;
- if you are considering undertaking any activities involving automated processing including profiling or automated decision-making;
- if you need help complying with applicable law when carrying out direct marketing activities;
- if you need help with any contracts in relation to data protection or privacy;
- if you need help in relation to sharing personal data with third parties (including service providers).

## Personal data protection principles

We adhere to the principles relating to processing of personal data set out in Data Protection Legislation which require personal data to be:

- processed lawfully, fairly and in a transparent manner (“Lawfulness, Fairness and Transparency”);
- collected only for specified, explicit and legitimate purposes (“Purpose Limitation”);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (“Data Minimisation”);
- accurate and where necessary kept up to date (“Accuracy”);
- not kept in a form which permits identification of Individuals for longer than is necessary for the purposes for which the data is processed (“Storage Limitation”);
- 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”);
- not transferred to another country without appropriate safeguards being in place (“International Transfer Limitation”);
- made available to Individuals and with Individuals able to exercise certain rights in relation to their personal data (“Individual's Rights and Requests”).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above ("Accountability"). See separate sections below on each of the above principles.

## Lawfulness, Fairness, Transparency (including privacy policies)

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Individual.

### Lawfulness and fairness

You may only collect, process and share personal data fairly and lawfully and for specified purposes without adversely affecting the Individual.

Data Protection Legislation **only allows processing for specific purposes**, which must be **documented and notified to the Individual**. In our case this is done in our Privacy Policy. Some of the permitted specific purposes are set out below (there are also a few less relevant to us, but check the ICO Guide for the full list or if unsure and wanting more detail). We have reordered these for relevance to us:

- to pursue our legitimate interests (see notes below)
- the processing is necessary for the entry into or performance of a contract with the Individual;
- to meet our legal compliance obligations;
- the Individual has given his or her consent (see notes below);
- to protect the Individual's vital interests (such as a life or death situation);

For licensees: You must identify and document the legal ground above being relied on for each processing activity. This can be done within your Privacy Policy (see separate section below on Transparency).

### Notes On Our Legitimate Interests

You can use personal data for our legitimate interests. This is a broad and commonly used category and encompasses many normal uses of personal data (which can include marketing, subject to the section below) and can include the decision to pass data to service providers, as examples only.

However, whenever you are using this as the basis for processing personal data, you must actively think about the effects on the Individual and must weigh this up against our legitimate interests in a "balancing act". You may not use this basis if our legitimate interests are overridden because the processing prejudices the interests or fundamental rights and freedoms of Individuals.

### Notes on consent

You must **avoid using consent wherever possible**, no matter what may have been the practice in the past, or what you see other businesses doing. There is a lot of bad advice and practice even within large companies, but do not copy it. Consent makes our life complicated (because of the requirements below) and always needs to be able to be withdrawn. It is therefore not appropriate for anything where you need the personal data for any essential part of performing services or employing anyone. Very often, there are better justifications for the processing such as legitimate interests, contract or legal compliance. However, sometimes consent will indeed be needed (see the section on Direct Marketing for example).

An Individual consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. **Consent requires affirmative action** so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters. See the definition of consent.

Individuals must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the Individual first consented.

You need to record evidence of consent captured and keep records of all consents so that you can demonstrate compliance with consent requirements. This is important legally.

When processing sensitive data, we will usually rely on a legal basis for processing other than consent if possible, but if you do rely on it, then it must be explicit consent (see the ICO Guide). Where explicit consent is relied on, you must issue a specific privacy notice to the Individual to capture explicit consent.

### **Transparency (notifying Individuals) including Privacy Policies**

Data Protection Legislation requires controllers to provide detailed, specific information to Individuals depending on whether the information was collected directly from Individuals or from elsewhere. The information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language that can be easily understood.

If you are collecting personal data from Individuals, directly or indirectly, then you must provide Individuals with a privacy notice (we refer to it as a privacy policy). The notice may be by link to your website's privacy policy if the policy is on there and if providing a link is sufficient in the circumstances. The policy or notice must include all the information required by Data Protection Legislation including the identity of the controller and contact details and how and why you will use, process, disclose, protect and retain that personal data. The privacy notice which must be presented when the Individual first provides the personal data. For that reason, you need to think about the earliest point at which people may provide personal data and ensure that they are given a copy of the privacy policy at that point. For example, you should have a link to your privacy policy in your email footer, since personal data may come by email.

When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the Individual with all the information required by Data Protection Legislation as soon as possible after getting the data. You must also check that the personal data was collected by the third party in accordance with Data Protection Legislation and on a basis which contemplates our proposed processing of that personal data. As an example, you cannot buy marketing lists with personal contact details unless the people on the list consented to receiving marketing from us.

Note to our licensees: we suggest splitting your privacy policy at least into two separate versions, one for clients / general users and one for personnel. We may have provided you with precedents for some or all policies, but they are your responsibility by law and it is up to you and your lawyers to adapt them to be correct for your own business and any applicable data protection legislation where you are based.

### **Purpose Limitation**

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. You cannot use personal data for new, different or incompatible purposes from those disclosed when the data was obtained unless you have informed the Individual of the new purposes and (if necessary) got their consent.

### **Data Minimisation**

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You may only process personal data to the extent that your role in your job requires it. You cannot process personal data for any reason unrelated to your job duties.



You may only collect personal data required for the purpose: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes and do not collect it otherwise. You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised as soon as possible (see Storage Limitation below).

You should be particularly careful not to collect sensitive data unless you really need it. If you do collect it, you will have additional obligations under data protection law in relation to processing it and will need to research and comply with those. In addition, in our business there is no reason to collect personal data from anyone under the age of 18 years old and you should not do so.

## Accuracy

Personal data must be accurate, complete and, where necessary, kept up to date. It must be corrected or deleted without delay if inaccurate (including if an Individual notifies a change or correction to you) or out of date. You must check accuracy of personal data at the time of collection and then at regular intervals.

## 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 may have specific retention policies to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time. Otherwise, follow the guidelines below and any applicable legislation.

You must not keep personal data in a form which permits the identification of the Individual for longer than needed for the legitimate business purpose or purposes for which we originally collected it (which may include needing to retain it to satisfy any legal, accounting, tax or reporting requirements).

You must ensure Individuals are informed of the period for which data is stored and how that period is determined in any applicable privacy policy.

You must take all reasonable steps to destroy or erase from our systems all copies (including back-up copies and online copies) of personal data that is no longer needed. This includes requiring third parties to delete that data where applicable.

## Security, Integrity and Confidentiality

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

We must 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. We must regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. We may instigate specific programmes and certifications for information security.

Everyone is responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. You must exercise particular care in protecting sensitive data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of personal data from the time of collection to the time of destruction. You may only transfer personal data to outsiders including service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place.



You must protect the confidentiality, integrity and availability of personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it;
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed; and
- **Availability** means that authorised users are able to access the personal data when they need it for authorised purposes.

You must comply with all applicable aspects of any information security policy or programme of ours and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain. If you are a licensee, you must also implement and maintain your own safeguards.

## Reporting a Personal Data Breach

Data Protection Legislation requires controllers to notify any personal data breach to the applicable data protection authority or regulator and, in certain instances, the Individual.

Our DPM is the one who will deal with any suspected personal data breach and will notify Individuals or any applicable regulator where we are legally required to do so. If you are a licensee, you should ensure that your DPM has training to do the same or that you have an external specialist to consult.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself and do not yourself notify anyone. **Immediately contact the DPM** and give as much detail as possible of the incident and then follow their instructions (they may also liaise with external legal advisers and / or information security or data protection specialists).

## International Transfer Limitation

Data Protection Legislation restricts data transfers to countries outside the EEA / UK to ensure that the level of data protection afforded to individuals by Data Protection Legislation is not undermined. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer personal data outside the EEA / UK if permitted by law, which at present would mean that one of the conditions below applies. However, please bear in mind that the situation changes depending on legal decisions (such as in 2020 when the US Privacy Shield was held to be inadequate) and European Commission and ICO decisions, so it is important for you to check the websites of the European Data Protection Board and the ICO or your home country data protection authority for updated guidance and instructions, or ask your own lawyer if unsure.

- the European Commission / ICO has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the Individual's rights and freedoms; at the date of this Standard, the list from the European Commission can be found here: [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en);
- 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 DPM;
- the Individual has provided Explicit consent to the proposed transfer after being informed of any potential risks; in our case, we will almost never rely on this condition

- the transfer is necessary for another reason permitted under Data Protection Legislation such as the performance of a contract between us and the Individual, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Individual if physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest (we do not recommend using this basis and detailed advice would be needed).

For the conditions that we use at the date of this Standard, please see our privacy policies. If you are a licensee, you will need to adapt your own policies to refer to countries where you transfer personal data, and which conditions or basis applies.

## Individuals' Rights and Requests

Individuals have rights when it comes to how we handle their personal data, which may vary depending on their location and residency. See the ICO Guide (for the UK) or your data protection authority website for more details and go through our privacy policies aimed at Individuals and setting out a summary of their rights. In the UK and EEA these rights include rights to:

- withdraw consent to processing at any time (but only in the limited circumstances where we used consent as the basis for processing their personal data);
- prevent our use of their personal data for direct marketing purposes;
- receive certain information about the Data controller's processing activities;
- request access to their personal data that we hold (sometimes called a "Subject Access Request");
- 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;
- restrict processing in specific circumstances;
- challenge processing done on the basis of our legitimate interests or in the public interest;
- request details of the basis under which personal data is transferred outside of the EEA / UK;
- object to decisions based solely on automated processing, including profiling;
- prevent processing that is likely to cause damage or distress to the Individual or anyone else;
- be notified of any personal data breach likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority;
- 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.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

You must **immediately forward any Individual request you receive to the DPM** who will guide you on the process to respond to Individuals' requests. You and your personnel should be alert and trained to recognise the exercise by an Individual of any of their rights. The Individual does not have to use particular wording and cannot be forced to follow any particular procedure or fill in particular forms to exercise their rights, so watch out for requests on social media or emails for example.

## Accountability and Record Keeping

The controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

You must have adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including (in the UK or EEA, but check for anywhere else):

- appointing a suitably qualified DPO (where necessary) or otherwise a DPM; **do not refer to any member of your personnel as the Data Protection Officer or DPO** unless you are legally required to have one (check the ICO Guide if unsure), because it incurs legal obligations and liabilities; instead you can call the responsible person the DPM / Data Privacy Manager or similar name;
- implementing privacy by design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of Individuals;
- integrating data protection into internal documents including this Standard, privacy policies and any other policies, standards, procedures, guidelines, templates or contracts;
- regularly training all personnel and conducting audits or reviews of processes (see section below).

Data Protection Legislation requires keeping full and accurate records of all data processing activities. You must keep and maintain accurate records reflecting our processing including records of Individuals' consents and procedures for obtaining them.

These records should include, at a minimum, the name and contact details of the controller and the DPM, clear descriptions of the personal data types, Individual types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, transfers, retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

## Training and Audits

All personnel must receive at least sufficient regular obligatory training to enable them to comply with Data Protection Legislation, this Standard and our privacy policies. Managers (especially the DPM and any deputy for the DPM in case of absence) should get more detailed training for example on Individuals' rights, consent, legal basis, DPIA and personal data breaches and should also consider appointing external experts if needed. You must **maintain a record of training** of all personnel.

You must regularly test the privacy measures implemented and conduct periodic reviews or audits to assess compliance, including using results of these to demonstrate effort for improvement.

## Privacy by Design

Privacy by design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Data Protection Legislation and incorporating this compliance into all our business practices, processes and procedures. We are required by law to evaluate and implement privacy by design measures. Examples include using pseudonymisation or anonymisation of data if possible (the latter means that it is no longer personal data if an Individual could no longer be identified). See the ICO Guide for more examples and best practice.

You must assess what privacy by design measures can be implemented on all programmes, systems or processes that process personal data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of likelihood and severity for rights and freedoms of Individuals from the processing.

## Data Protection Impact Assessment (DPIA)

Data controllers must conduct DPIAs in respect to any high-risk processing. If you need to conduct a DPIA, contact your DPM for advice or to pass you to an external expert for help (or consult the ICO Guide). You should conduct a DPIA (and discuss your findings with the DPM) when implementing major system or business change programs involving the processing of personal data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing including profiling and automated decision making (see below);
- large-scale processing of sensitive data;
- large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the processing, its purposes and the controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals;
- the risk mitigation measures in place and demonstration of compliance.

## Automated processing (including profiling) and Automated Decision-Making

Automated processing in the context of Data Protection Legislation is any form of automated processing of personal data to evaluate certain aspects relating to an Individual, for example to analyse or predict aspects of that Individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing. You must provide Individuals with information about any automated processing and their rights.

Automated Decision-Making is when a decision is made based solely on automated processing. Data Protection Legislation generally prohibits Automated Decision-Making when a decision has a legal or similar significant effect on an individual with certain specific exceptions and conditions. Our own policy is never to do Automated Decision-Making and in particular never to apply it to sensitive data (which has further requirements). You should assess your systems to ensure that decisions that have a legal or similar effect (such as a decision to employ someone) are not made without significant meaningful human input.

## Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers. In summary, the only exception and only time that you can send direct marketing without prior consent is when sending marketing to existing customers about similar products or services. Even then, which is what is known as "soft opt-in", you must always give the Individual a chance easily to opt out of marketing when first

collecting the details and in every subsequent message. For example, when we use Mailchimp, that opt-out should always be available.

For all other direct marketing, you need active prior consent on an “opt-in” basis, without check boxes being pre-filled. You must record this consent and check again at regular intervals. The consent / right to object to direct marketing must be explicitly offered to the Individual in an intelligible manner so that it is clearly distinguishable from other information. For example, it cannot be mixed in with other terms and conditions or other consents.

An Individual's objection to direct marketing must be promptly honoured (and remember that they can object by any communication method they wish). If an Individual 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.

## Sharing personal data

You may only share the personal data we hold with other personnel or companies (even if related group companies) if the recipient has a job-related need to know the information and the transfer complies with any applicable international transfer restrictions.

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contracts are in place. You must never sell personal data to anyone. By law, **you will personally be in breach and subject to reporting and fines** if you copy or share any personal data collected by the business (for example actual or potential client contact lists or databases) outside of the business or for any use other than the use and for the company for which it was collected. You may only share the personal data we hold with third parties, such as our service providers, if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the personal data complies with our privacy policy and, if required, the Individual's consent has been obtained (check with your DPM if not sure);
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable international transfer restrictions; and
- an executed written contract that contains Data Protection Legislation-approved third party clauses has been obtained (such as the European Commission controller to process clauses).

If at all unsure, contact your DPM or the ICO guide before sharing any personal data, and keep records.

## Our Role as a Data controller or processor

We are the controller and responsible for personal data where we collected that data for our own business purposes or where we are the person who controls and decides about its processing. Where we perform services for someone else who originally collected the personal data, we are the "processor" of that data. From our side as a processor, we must comply with all requirements on data processors in Data Protection Legislation and with our privacy policy. These include that we must:

- process the personal data only on the documented instructions of the controller;
- enter into a written contract or undertake to comply with written contractual clauses with the controller with regard to the data processing;
- only use personnel who have a duty of confidentiality with regard to the data;

- comply with security obligations equivalent to those imposed on the controller by law;
- notify the controller of any breach in relation to the personal data shared by the controller;
- enlist a sub-processor only with the prior permission of the controller.

## Changes to This Standard and Your Suggestions

We keep this Standard under review. The date that it was last updated is set out below.

As a result of our reviews, we reserve the right to make changes to this Standard from time to time. The current version is the one at the relevant time on our internal website for licensees and personnel.

*© EXB Ltd 2020 – no copying permitted*

Version Date: 23.01.21