



**Usel**

# **Data Protection Policy (GDPR 2018)**

## DOCUMENT MANAGEMENT

The purpose of this section is to provide details of the official, versions and controls relating to the management of the Data Protection (GDPR 2018) Policy.

### KEY PERSONNEL

| Role    | Name               | Grade                      | Responsibility |
|---------|--------------------|----------------------------|----------------|
| Author  | Patrice Devine     | Compliance Manager         | Draft          |
| Manager | Sarah-Jane Mowbray | Head of Corporate Services | Review         |
| Owner   | Board              | -                          | Approval       |

### DOCUMENT HISTORY

| Version | Date       | Reason for update                         |
|---------|------------|---|
| 1.0     | Feb 2018   | Draft for Review                          |
| 2.0     | April 2018 | Review from Data Protection Officer (DPO) |
|         |            |   |

## 1. Introduction

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access during their work. This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

## 2. Definitions

|                                |   |
|--------------------------------|---|
| <b>Business purposes</b>       | <p>The purposes for which personal data may be used by us:</p> <p>Personnel, administrative, financial, regulatory, payroll and business development purposes.</p> <p><i>Business purposes include the following:</i></p> <ul style="list-style-type: none"><li>➤ Compliance with our legal, regulatory and corporate governance obligations and good practice</li><li>➤ Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests</li><li>➤ Ensuring business policies are adhered to (such as policies covering email and internet use)</li><li>➤ Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking</li><li>➤ Investigating complaints</li><li>➤ Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments</li><li>➤ Monitoring staff conduct, disciplinary matters</li><li>➤ Marketing our business</li><li>➤ Improving services</li></ul> |
| <b>Personal data</b>           | <p>Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.</p> <p><i>Personal data we gather may include, but is not limited to: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.</i></p>  |
| <b>Sensitive personal data</b> | <p><i>Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.</i></p>   |

## 3. Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our Data Protection Officer, [Geraldine Fahy – dataprotection@usel.co.uk] has overall responsibility for the day-to-day implementation of this policy.

#### **4. Our procedures**

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

#### **5. The Data Protection Officer's responsibilities:**

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Usel
- Checking and approving with third parties that handle the company's data and any contracts or agreement regarding data processing

#### **6. Responsibilities of the IT Manager**

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

#### **7. Responsibilities of the Marketing & Business Development Manager**

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

#### **8. The processing of all data must be:**

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities

#### **9. Our Policy contains a Privacy Notice to clients on data protection.**

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as employers and suppliers

- Provides that customers have a right of access to the personal data that we hold about them

## **10. Sensitive personal data**

In most cases where we process sensitive personal data; we will require the data subject's *explicit* consent to do this, unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

## **11. Accuracy and relevance**

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, [Geraldine Fahy – dataprotection@usel.co.uk]

## **12. Your personal data**

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the DPO so that they can update your records with the necessary departments.

## **13. Data security**

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

## **14. Storing data securely**

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it. No notes referring to individuals must be transported on paper outside of the business at any time.
- In cases when data is stored digitally, this should only be accessed using ICT equipment and approved applications supplied by Usel's ICT department. Staff should not access any personal data on their own personal device.
- Printed data should be shredded when it is no longer needed using the supplied shredding facility within Usel
- Data stored on a computer should be protected by strong passwords that are changed regularly. These passwords should not be written down.
- The DPO must approve any cloud facility used to store data and all staff must only use the approved storage facility.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

## **15. Data retention**

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

## **16. Transferring data internationally**

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the DPO.

## **17. Subject access requests**

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

Please contact the DPO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

## **18. Training**

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through in-house training initially, then online refresher training annually.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

## **19. GDPR provisions**

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018

## **20. Conditions for processing**

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

## **21. Justification for personal data**

We will process personal data in compliance with all six data protection principles:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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 not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

## **22. Consent**

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

## **23. Criminal record checks**

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

## **24. Data portability**

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

## **25. Right to be forgotten**

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

## **26. Privacy by design and default**

Privacy by design is an approach to project/promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

## **27. International data transfers**

No data may be transferred outside of the EEA (European Economic Area) without first discussing it with the DPO. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

## **28. Data audit and register**

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

## **29. Reporting breaches**

All employees have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO and Department for Communities (where appropriate) of any compliance failures that are material either in their own right or as part of a pattern of failures

A form has been developed to facilitate this and can be found in the internal HR Documents folder. In addition, feel free to contact our DPO and/or line management if you wish for any clarification

## **30. Monitoring**

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

## **31. Consequences of failing to comply**

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

