DATA PROTECTION POLICY & STANDARDS

Date Issued: 1 March 2018

Version 1.0

Document control	
Version	1.0 (for adoption)
Reviewer	Jamie Lynch
Date	1.3.2018

CONTENTS

1. INTRODUCTION

This Data Protection Policy & Standards ("Data Protection Policy") sets out how Interserve Plc and all Interserve Divisions ("we", "our", "us", "Interserve") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Data Protection Policy 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 Data Protection Policy applies to all Interserve Staff ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on Interserve's behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for Interserve to comply with applicable data privacy laws. Your compliance with this Data Protection Policy is mandatory.

This Data Protection Policy shall be adopted by all Interserve Divisions. In addition, the Interserve Division you work for may publish Related Policies and Privacy Guidelines to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

This Data Protection Policy (together with Related Policies and Privacy Guidelines issued by the Interserve Division you work for) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Citizen Services Divisional Data Protection Officer.

2. INTERPRETATION

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.

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.

Data 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 Data

Controller of all Personal Data relating to Interserve Staff and Personal Data used in our business for our own commercial purposes.

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. A 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.

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.

Interserve Division: the business of Interserve Plc is conducted by Group Centre and its five divisions; Construction, Equipment Services (RMD Kwikform), International, Investments and Citizen Services, and Support Services, each are an Interserve Division.

Interserve Staff: all employees, workers contractors, agency workers, consultants, directors, members and others.

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 Sensitive 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 Guidelines: privacy/GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies.

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 Interserve 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 simply 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.

Related Policies: policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data.

Sensitive 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, and Personal Data relating to criminal offences and convictions.

3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in Interserve 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. Interserve is exposed to potential fines of up to 4% of our total worldwide annual turnover for any failure to comply with the provisions of the GDPR.

Each of Interserve's Divisions is responsible for ensuring that all Interserve Staff which it employs or engages comply with this Data Protection Policy, and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Citizen Services Divisional Data Protection Officer is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines.

4. PERSONAL DATA PROTECTION PRINCIPLES

Interserve adheres 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

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.1 Lawfulness and fairness

Interserve may 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.

The GDPR allows Processing 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; or

(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. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

We will implement processes to identify and document the legal ground being relied on for each Processing activity we undertake.

5.2 Consent

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject 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.

Data Subjects 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 we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers (i.e. where the Personal Data is being transferred to a country outside of the European Economic Area).

Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Personal Data. Where Explicit Consent is required, we must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

We will implement measures to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

5.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

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 including the identity of the Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6. 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.

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

7. DATA MINIMISATION

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

Interserve Staff may only Process Personal Data when performing their job duties requires it. Interserve Staff cannot Process Personal Data for any reason unrelated to their job duties.

We must not collect excessive Personal Data and need to ensure any Personal Data collected is adequate and relevant for the intended purposes.

Each Interserve Division must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with its data retention guidelines.

8. ACCURACY

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

Each Interserve Division must ensure that the Personal Data it uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it is collected. As a minimum, this will involve checking the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Further, all reasonable steps must be taken to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

Personal Data must not be kept 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.

Each Interserve Division will maintain its own retention policies and procedures to ensure that stored Personal Data is regularly reviewed, and where necessary, deleted in compliance with this requirement. This includes requiring third parties to carry out such action where that third party is storing Personal Data on our behalf.

It is important to ensure that Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice which the Interserve Division publishes.

10. 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.

10.1 Protecting Personal Data

Interserve 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.

Each Interserve Division shall be responsible for protecting the Personal Data it holds and 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. It will be important to exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies Interserve puts in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

We may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

We must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) 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 our Information Security Policies and Procedures (as published on IRIS) and not attempt to circumvent the administrative, physical and technical safeguards which Interserve has implemented and maintains.

10.2 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator (in the United Kingdom, this is the Information Commissioner's Office) and, in certain instances, the Data Subject.

Each Interserve Division shall put in place procedures to deal with any suspected Personal Data Breach and notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately follow the Personal Data Breach Response Plan.

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. 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.

Interserve shall not transfer Personal Data to a location outside the EEA unless 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 Citizen Services Divisional Data Protection Officer;

(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.

Each Interserve Division must implement measures to give effect to the exercise of these rights. As part of these measures, it will be important that processes are in place to verify the identity of an individual requesting data under any of the rights; never allow third parties to persuade you into disclosing Personal Data without proper authorisation.

13. ACCOUNTABILITY

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

13.1 It is the responsibility of each Interserve Division to put in place adequate resources and controls to ensure, and to document, GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;

(d) regularly training Interserve Staff on the GDPR, this Data Protection Policy, any Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. Each Interserve Division must maintain a record of training attendance by Interserve Staff; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.2 Record keeping

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

Each Interserve Division must keep and maintain accurate corporate records reflecting its Processing activities, including records of Data Subjects' Consents and procedures for obtaining Consents.

As a minimum, these records should include the name and contact details of the Data Controller [*the DPO / alternative role with data privacy compliance responsibility*], clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.3 Training and audit

We are required to ensure all Interserve Staff 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.

Each Interserve Division must regularly review all the systems and processes under its control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

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

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Each Interserve Division must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

We must also conduct DPIAs where high risk Processing is taking place.

Each Interserve Division must implement procedures to conduct a DPIA (and discuss your findings with the Citizen Services Divisional Data Protection Officer when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) Automated Processing including profiling and ADM;

(c) large scale Processing of Sensitive Personal Data; and

(d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

You must comply with Interserve's guidelines on DPIAs and Privacy by Design.

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

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Personal Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Personal Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when we first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with Interserve's guidelines on profiling or ADM.

13.6 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.

You should only share the Personal Data we hold with another employee, agent or representative of Interserve if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We may 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) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, 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;

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

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

You must comply with Interserve's guidelines on sharing data with third parties.

14. CHANGES TO THIS DATA PROTECTION POLICY

We reserve the right to change this Data Protection Policy at any time without notice so please check back regularly to obtain the latest copy of this Data Protection Policy.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where Interserve operates.