Table of Contents

1 Introduction

InContrast is committed to safeguarding the privacy of InContrast Customers, Suppliers and Employees 'Personal Identifiable Information (PII)' in all of its activities.

As of 25th May 2018, the European General Data Protection Regulation (GDPR) is the primary legislation covering the protection of PII. This Policy describes the processes in place in InContrast that ensure that compliance with GDPR is maintained.

2 Scope

The scope of GDPR within InContrast covers all activities where formal records that include PII are made as part of the operation of InContrast. Specifically:

2.1 In scope

The following are in scope:

- Maintaining and Enhancing our Services
- Complying with contractual obligations
- Account and customer management,
- Marketing,
- Support and system security,
- Audits,
- Detect and prevent fraud
- Legal compliance.
- Quality Incident Records that may contain some PII
- Employees data;

2.2 Out of scope

The following are not in scope as they are not part of any formal processes:

- Notes made as part of prospective enquiries
- Details already in the public domain

3 Roles, Responsibilities and Awareness

3.1 Awareness

Awareness of the responsibilities and the requirements of the GDPR legislation will form part of the annual training cycle of all senior management.

3.2 InContrast Member Roles and Responsibilities

All employees are responsible for ensuring the correct handling of PII, should they be involved with it.

The small volume of data involved in InContrast activities does not require the appointment of a dedicated DPO, however we have appointed a Data Controller.

The role specific responsibilities are detailed in following table:

Role	Responsible for
Data Controller (as shown in the privacy policy)	1. Ensuring that this policy is adhered to. 2. Maintaining the InContrast registration with the ICO. 3. Ensuring all employees are made aware of the GDPR requirements and maintain the associated competency. 4. Maintaining awareness of the data processing requirements placed on InContrast by the GDPR legislation through the training provided by InContrast. Ensuring that all data collected and processed by InContrast employees is collected and processed in accordance with this policy. 5. Providing only the PII data that has been identified as pertinent for normal business. 6. Cleaning up records in accordance with the specified retention policies. 7. Ensuring all InContrast records are safely secured in the defined storage.

3.3 Organisational Data Processing Roles

InContrast performs several of the recognised “roles”, depending upon the context of the activity.

3.3.1 InContrast in its own right

InContrast fulfils the roles of:

- Data Controller
- Data Processor

4 Monitoring and Reporting

Monitoring of and reporting on data processing activities within InContrast will become part of the InContrast management activities.

5 The Specifics

5.1 Data Processing Activities

A number of discreet data sets have been identified within the activities of InContrast, where data processing takes place. Each of these has unique characteristics, resulting in differing requirements for processing, retention etc..

They are detailed below in sections 5.1.1 to 5.1.5.

5.1.1 Customer Details

These take the form of Electronic Records returned to InContrast following interaction with any customer

Activity	Description
Source	Customers
Collected	Via an electronic Customer form.
Lawfulness	Collected using a new Customer form as the legal basis and is used to maintain and enhance our services.
Purposes	Customer Records and Financial information. Complying with contractual obligations. Account and customer management, Marketing, Support and system security, Audits.
	Detect and prevent fraud.
Retention Policy	7 Years after cessation of relationship.
InContrast Role	Controller and Processor
Security Measures - Storage	Paper hard copies – locked away in the Commercial Office.
	Electronic - Stored within InContrast owned and managed database(s) specifically designed for the collection, storage and security of such data.
Associated Processes	None required

5.1.2 Suppliers Details

These take the form of Electronic Records returned to InContrast following interaction with any Supplier

Activity	Description
Source	Suppliers
Collected	Via an electronic Suppliers form.
Lawfulness	Collected using a new Supplier form as the legal basis and is used to maintain and enhance our services,
Purposes	Suppliers Records and Financial information Complying with contractual obligations. Account and customer management, Marketing, Support and system security, Audits,
	Detect and prevent fraud,
Retention Policy	7 Years after cessation of relationship
InContrast Role	Controller and Processor
Security Measures - Storage	Paper hard copies – locked away in the Commercial Office.
	Electronic - Stored within InContrast owned and managed database(s) specifically designed for the collection, storage and security of such data.
Associated Processes	None required

5.1.3 Quality Incident Records

Activity	Description
Source	InContrast and Customers
Collected	By PM's and Quality Dept dealing with any Quality issues by completing entries in the database system created for such purpose.
Lawfulness	Legitimate Interests of InContrast to carry out investigation into Quality Incidents.
Purposes	Investigation into Quality Incidents.
	Non Conformities and Preventative actions.
	Reporting.
	Exercise or defence of legal claims.
	Obtain or maintain management of risk.

Retention policy	Until 7 years after the incident.
InContrast Role	Controller and Processor.
Storage	Stored within InContrast owned and managed database(s) specifically designed for the collection, storage and security of such data.
Associated Processes	Clean up of data in accordance with the retention period (6.1.1)

5.1.4 Employees Details

These take the form of "New Employee form" following recruitment.

Activity	**Description**
Source	"New Employee Form"
Collected	Via a paper "New Employee form" held at InContrast
Lawfulness	Collected using Employees Information as the legal basis and is a mandated requirement of InContrast Employees. Legitimate Interests of InContrast in order to maintain accurate records, salary payments and conform to legal requirements.
Purposes	Maintain accurate records.
	Wages.
	Satisfy legal requirements.
	Communications to Employees.
Retention Policy	7 Years after cessation of employment.
InContrast Role	Controller and Processor
Security Measures - Storage	Paper – locked cupboard; medical team access as defined by the Medical Officer.
	Electronic - Stored within InContrast owned and managed database(s) specifically designed for the collection, storage and security of such data.
Associated Processes	Clean up of data in accordance with the retention period (6.1.2)

6 Processes

The following processes are in place:

6.1.1 Clean up – Employee Data

1. The appropriate authorised personnel can mark employees as no longer employed. Once this is done the retention policy is enforced.

6.1.2 Removal of Consent (where consent is the legal basis)

1. In order to remove consent an individual must send an email to InContrast giving any information to adequately identify themselves (at a minimum a name and email address)
2. The data shall be removed within 14days and confirmation sent to the requestor.

6.1.3 Amendment of Data

1. In order to have data amended an individual must send an email to InContrast giving any information to adequately identify themselves (at a minimum a name and email address) and the data that they require amending.
2. This will be reviewed and a decision will be made as to whether the data can/should be amended due to an accuracy issue.
3. Where required, the data shall be amended within 14days and confirmation sent to the requestor.

6.1.4 Right to be Forgotten

1. In order for an individual to exercise their right to be forgotten the individual must send an email to InContrast giving any information to adequately identify themselves (at a minimum a name and email address)
2. All data shall be removed within 14days (subject to the provisions for legal hold as given in the privacy policy) and confirmation sent to the requestor.

6.1.5 Subject Access Request

1. Subject Access Requests (SAR) must be made by the individual concerned (a 3rd party may not undertake a SAR) by email to InContrast giving any information to adequately identify themselves (at a minimum a name and email address)
2. Once confirmed as a valid and genuine request the data will be supplied within 30days. However if the request is more complex or involves a large amount of data then InContrast will provide the data within 60days and will inform the requestor of this within 7 days of the request.
3. Where InContrast believes that the frequency of requests is unreasonable then a data processing charge of £10.00 will be levied.

End of Document