Integrum Services Ltd
Office 204, Access Building,
92 Oldfields Road, Sutton SM1 2NU
Surrey.  SM4 5HP
Tel - 0208 9147894
office@integrumservices.co.uk
www.integrumservices.co.uk

Registered in England and Wales 10937646

**Privacy Policy**

**March 2019**

## Integrum Services Ltd's Privacy Notice

Here at the Integrum Services Ltd we know how important it is to keep your personal data safe, that's why we're committed to making sure that you receive the service you'd expect and that your privacy is protected every step of the way.

In this notice you'll discover exactly what information we collect from you and how we then use this to deliver our services, as well as your rights. It might not be something you're interested in, but it's really important you have a read and of course, let us know if you have any questions.

Integrum Services ('we' and 'us') means Integrum Services Ltd, together with any entity in which Integrum Services Ltd directly or indirectly has at least a 50% shareholding. Integrum Services Ltd uses a variety of trading names. We may transfer your personal information among the members of Integrum Services Ltd for the purposes contemplated in this privacy notice.

## So, how do we use your information?

When you buy a product or service through us, we'll collect some of your personal details, to make sure you have everything you need to make the most of our services. Please rest

assured that we'll only use this for administering your contract and to support the delivery of the services or products you've asked for.

Examples of the types of personal information we usually collect are:

- Name
- Address
- Telephone number (including mobile)
- Email address
- Date of birth
- Payment details (Direct Debit, credit/debit card number)
- Property type (flat, house etc.)
- Nature of Problem and Findings
- Any additional requirements such as large print or Braille documentation
- Details of any additional authorised parties who can manage your requirements on your behalf
- I.P. address for your device (if visiting our website or using our app)

The information requested during the application process is required to complete the sale of the product on offer and forms part of your contract with us. Unless otherwise stated, the information you provide will never be used for any other purpose without your permission. If any of the data is missing from the application form or is incorrect, we may not be able to process your request.

**Using information provided by third parties**

We sometimes use data from third parties or publicly available sources such as Experian, the edited electoral roll or the deceased preference service. Using this data helps us to ensure that our records are accurate and up to date by filling in any gaps on an address or clarifying vanity addresses and house numbers. It also allows us to remove anyone from our mailings that has passed away.

We also use data for marketing purposes. Any data we use in this way is thoroughly checked by both the supplier and our own internal teams to ensure that the correct marketing permissions are in place and that the data is being used fairly.

**Keeping and storing your data**

If you're a current or past customer, we'll keep a copy of your personal details for no longer than 6 years, from the time your active relationship with us ends. Holding on to data allows us to keep accurate records for tax purposes and to handle any future complaints. All other personal data used for prospecting and quotation requests is kept for a maximum of 90 days, unless otherwise required by law.

Some of the data that we collect may be transferred to and stored at a destination outside the European Economic Area ('EEA'), for example some of our IT systems are run on servers hosted in the USA. We take all steps reasonably necessary to ensure that your data is treated in accordance with this privacy notice and applicable privacy laws.

**Sharing your data with third parties**

We often work with a number of carefully selected third parties, who introduce us to their customers, so we can promote the products and services we offer.

If you've been introduced to us through one of our partners, we may share details of the products and services you've purchased with them. Sharing data in this way helps us resolve individual complaints and helps us ensure that we're offering the right products, to the right people.

We respect your privacy and that's why we don't give your data to any third parties for marketing purposes. However, on occasion and in addition to the above, we may pass your information to a limited number of third parties for the following reasons:

- To deliver the services you've asked for, which might include giving information to members of your family, household, or other people who have an interest in the property, for instance, landlords or letting agents
- For legal or regulatory purposes including fraud prevention
- If we buy or sell any business or company assets

**We'll always keep you in the loop**

Whenever we collect your personal information we'll give you the opportunity to let us know how you'd like us to get in touch in the future. We promise not to inundate you with marketing messages, but we also understand if you'd prefer not to receive anything from us.

If you've asked us to send you marketing material, you can change your mind at any time by contacting us using the details in the Contact Us section. You'll also find an unsubscribe link at the bottom of every marketing email we send to you.

If you've given us an email address you may receive messages related to the management of your policy via email, which include policy and renewal documents. If you'd prefer not to receive these messages in this way, just let us know and we'll be happy to provide them in paper form instead.

**Your rights matter**

If you'd like to see the personal information that we hold about you, you can request a copy any time. If you find that this information is incorrect you can ask for it to be updated. Or, if you believe the information is being processed without a legal basis, you can ask us to stop or request that it's deleted from our systems.

To action any of the above, send an email to: office@integrumservices.co.uk or alternatively you can write to us at:

Integrum Services LTD, 113 London Road, Morden, Surrey. SM4 5HP

We won't ever charge you for a copy of your personal data but we may ask you for proof of your identity before we disclose any information. Once we've seen this, we'll send you a copy of the personal data we hold within 30 days. In addition, if you decide to move away from us for any reason, you can also request for your personal data to be transferred to a new provider on your behalf.

**Customer profiles**

We carry out something called 'profiling' so we can understand the needs, behaviours and socio-demographic characteristics of our customers. This helps us make sure that we're offering the right products and services to the right people, for example, not offering commercial products to domestic customers or products to people living in sheltered accommodation, who don't need our services. Profiling also means we can tailor our offerings to current customers, enhancing the potential benefits of being a customer.

**Contact us**

**General Enquiries/Data Controller**

Integrum Services Ltd,

Tel – 0208 9147894

https://www.integrumservices.co.uk/contact

**Got any worries?**

If, at any time, you feel that we haven't processed your data fairly or you're not satisfied with how we've handled your personal information, you can contact the Information Commissioners Office, who will look into this for you. For full details about how to share any concerns you may have, visit www.ico.org.uk/concerns/

**Links to other Websites**

Any links to other websites are provided solely as pointers to information on topics that may be useful to the users of our website. Please remember that when you use a link to go from our website to another website, this privacy notice will no longer apply. Your browsing and interaction on any other website, including those which have a link on our website, are subject to that site's own rules and policies. We recommend that you read the rules and policies relating to that website before submitting any personal information.

**Updates**

This notice will be updated from time to time and we recommend that you check back regularly but we will notify you of any changes through our website. The version number and date released will always be listed below:

Version number: 1.0

# INTEGRUM SERVICES LTD

**Controlled Document**

| | |
|---|---|
| **Document Name:** | **Data Protection Policy** |
| **Document Reference Number:** | **POL1** |
| Document Version Number | 3 |
| Approved by Board: | 25 March 2018 |
| Review Schedule | Every two years |
| Next review due | March 2020 |
| Owner (Responsibility) | Peter Bowers-Davis – Managing Director |

**Document Description**

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how Integrum Services Ltd meets them. Note: until GDPR come into force on 28 May 2018 the current Data Protection Act 2000 will continue to apply.

**Implementation and Quality Assurance**

Implementation is immediate and this Policy shall stay in force until any alterations are formally agreed.

The Policy will be reviewed every two years by the Manging Director, sooner if legislation, best practice or other circumstances indicate this is necessary.

All aspects of this Policy shall be open to review at any time. If you have any comments or suggestions on the content of this policy please contact Peter Bowers-Davis peter@integrumservices.co.uk or at Integrum Services Ltd, 113 London Road, Morden, Surrey. SM4 6HU

# Data Protection Policy

## Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect it will replace the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applies from 25 May 2018 after a two-year transition period..

The 1998 Data Protection Act, which came into force on 1 March 2000, will continue to apply until the new General Data Protection Regulations come into force in May 2018.

The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points where they affect Integrum Services Ltd.

The Regulations cover both written and computerised information and the individual's right to see such records.

It is important to note that the Regulations also cover records relating to staff and volunteers.

All Integrum Services Ltd staff are required to follow this Data Protection Policy at all times.

The Managing Director has overall responsibility for data protection within Integrum Services Ltd but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

## Definitions

**Processing of information** – how information is held and managed.
**Information Commissioner** - formerly known as the Data Protection Commissioner.
**Notification** – formerly known as Registration.
**Data Subject** – used to denote an individual about whom data is held.
**Data Controller** – used to denote the entity with overall responsibility for data collection and management. Integrum Services Ltd is the Data Controller for the purposes of the Act.
**Data Processor** – an individual handling or processing data
**Personal data** – any information which enables a person to be identified

**Special categories of personal data** – information under the  Regulations which requires the individual's explicit consent for it to be held by the Charity.

## Data Protection Principles

As data controller, Integrum Services Ltd is required to comply with the principles of good information handling.

**These principles require the Data Controller to**:

1. Process personal data **fairly**, **lawfully and in a transparent manner.**
2. Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is **adequate**, **relevant and not excessive** for the purpose or purposes for which it is held.
4. Ensure that personal data is **accurate** and, where necessary, **kept up-to-date.**
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

## Consent

Integrum Services Ltd must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data covers information relating to:

1. The racial or ethnic origin of the Data Subject.
2. His/her political opinions.
3. His/her religious beliefs or other beliefs of a similar nature.
4. Whether he/she is a member of a trade union.
5. His/her physical or mental health or condition.
6. His/her sexual life.
7. The commission or alleged commission by him/her of any offence
8. Online identifiers such as an IP address
9. Name and contact details

10. Genetic and/or biometric data which can be used to identify an individual

Special categories of personal information collected by Integrum Services Ltd will, in the main, relate to service users' physical and mental health. Data is also collected on ethnicity and held confidentially for statistical purposes.

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

As a general rule Integrum Services Ltd will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Managing Director.

## Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face
- written
- telephone
- email.

Face-to-face/written

A pro-forma should be used.

Telephone

Verbal consent should be sought and noted on the case record.

E-mail

The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the

provision of that service, separate consent would be required if, for example, direct marketing of insurance products were to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record . The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by Integrum Services Ltd then the Service Co-ordinator should discuss with the Manager at the earliest opportunity.

## Ensuring the Security of Personal Information

Unlawful disclosure of personal information

1. It is an offence to disclose personal information ‘knowingly and recklessly’ to third parties.

2. It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.

3. Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis.

4. A client’s individual consent to share information should always be checked before disclosing personal information to another agency.

5. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Chief Executive or Services Manager should first be sought.

6. Personal information should only be communicated within Integrum Services Ltd’s staff and approved contractors on a strict need to know basis. Care should be taken

that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

## Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal / and/orspecial categories of personal data at home or in your car, the same care needs to be taken.

## Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home, or your client's home, to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents they should be carried out of sight in the boot of your car.

## Computers / Smart Phones / Data terminals

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computer monitors in public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, eg reception, you should lock your computer when leaving it unattended.

Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device must be password protected. All devices are enrolled on a MDM system which allows us to remotely disable and wipe and lost devices if required.

## Cloud Computing

When commissioning cloud based systems, Integrum Services Ltd will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

Integrum Services Ltd currently uses two cloud based data management systems to hold and manage information about its services and customers.

Microsoft
2 Kingdom Street Paddington
London
W2 6BD
Tel: +443448002400

Microsoft is a world-renowned provider of cloud based business software and storage solutions. Integrum Services Ltd is satisfied with the security levels in place to protect its data.

Freeagent –

One Edinburgh Quay
133 Fountainbridge
Edinburgh
Scotland United Kingdom
EH3 9QG
info@freeagent.com

Freeagent operates our full accounting system. Integrum Services Ltd is satisfied with the security levels in place to protect its data.

## Direct Marketing

The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. Integrum Services Ltd will not share or sell its database(s) with outside organisations.

Integrum Services Ltd holds information on our staff, suppliers and clients, to whom we will from time to time send copies of our newsletters, magazine and details of other activities that

may be of interest to them. Specific consent to contact will be sought from our staff, clients and other supporters, including which formats they prefer (eg mail, email, phone etc) before making any communications.

We recognise that staff, suppliers and clients for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their records and will be excluded from future contacts.

The following statement is to be included on any forms used to obtain personal data:
We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning 0208 9147894, writing to Peter Bowers-Davis peter@integrumservices.co.uk or at Integrum Services Ltd, 113 London Road, Morden, Surrey. SM4 6HU

## Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

A fuller Privacy Statement will also be published on our website.

## Personnel Records

The Regulations apply equally to customer, supplier and staff records. Integrum Services Ltd may at times record special categories of personal data as part of a staff member's contract of employment.

For staff Integrum Services Ltd to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Senior Management Team.

## Confidentiality

Further guidance regarding confidentiality issues can be found in our Confidentiality Policy.

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for Integrum Services Ltd should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked computer they should be saved onto a USB drive which should be password protected.

Workstations in areas accessible to the public, e.g. reception or trading office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

When sending emails to outside organisations,care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number, such as social services number, etc.) are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (eg on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. Enablers needing to take paperwork away from a client's must ensure that it is returned to the client's premises on the next visit.

If you are carrying documents relating to a number of clients when on a series of visits, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them into the clients premises. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain Integrum Services Ltd's contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's premises with the correct number of documents and that you haven't inadvertently left something behind.

## Retention of Records

Paper records should be retained for the following periods at the end of which they should be shredded:

- Client records – 6 years after ceasing to be a client.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Supplier records – 6 years after ceasing to be a supplier
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.
- Other documentation, should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

Computerised records to be anonymised 6 years after ceasing to have any services from us. (Anonymising will remove the personal and special categories of personal data but will not remove the statistical data.)

## What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to your line manager who will review our systems, in conjunction with the Senior Management Team and/or Quality Assurance & Systems Manager, to prevent a reoccurrence. The QA & Systems Manager should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner There is a time limit for reporting breaches to ICO so the QA & Systems Manager should be informed without delay.

Any deliberate or reckless breach of this Data Protection Policy by an may result in disciplinary action which may result in dismissal.

## The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

- Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).

- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.

- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
    - Where data is no longer necessary in relation to the purpose for which it was originally collected
    - When an individual withdraws consent
    - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - Personal data was unlawfully processed

- An individual has a right to restrict processing – where processing is restricted, Integrum Services Ltd is permitted to store the personal data but not further process it. Integrum Services Ltd can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

Integrum Services Ltd will not undertake direct telephone marketing activities under any circumstances.

Data Subjects can ask, in writing to the Chief Executive, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (Integrum Services Ltd) must comply with such requests within 30 days of receipt of the written request.

## Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

## Further Information

Further information is available at www.informationcommissioner.gov.uk

## Details of the Information Commissioner

The Information Commissioner's office is at:

Wycliffe House
Water Lane
Wilmslow

Cheshire SK9 5AF

Switchboard*:* 01625 545 700
Email: mail@ico.gsi.gov.uk
**Data Protection Help Line:** 01625 545 745
**Notification Line:** 01625 545 740