

# Privacy Policy Statement



This document sets out what information Independent Control Systems Limited (Iconsys) collects from visitors, how it uses the information, how it protects the information and your rights.

Iconsys is committed to ensuring your privacy is protected in accordance with Data Protection Standards.

Iconsys is using the following definition for Personal Data:

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.  <i>Personal data we gather may include: 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>
Sensitive personal data	<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 will only ever be carried out with the express permission of the individual.</i>

Iconsys may change this policy from time to time by updating this page. This policy is effective from 8<sup>th</sup> May 2018 but we ask you to check this page from time to time. Any updates or changes to the use of your personal data will be advised to you, prior to that change of use.

## Who We Are?

Independent Control Systems Ltd (Iconsys), Hortonwood 33, Telford TF1 7EX

## Contact Us

You can contact us by

Email : [dataprotection@iconsys.co.uk](mailto:dataprotection@iconsys.co.uk)

Phone : 01952 607300

Post: Independent Control Systems Limited, Technology House, Hortonwood 33, Telford TF1 7EX

## What services do we provide?

Iconsys provide a range of automation and control systems and solutions.

## What we collect

The specific information that we collect will vary depending on what services we provide you by way of contract, or what you either provide us explicitly e.g. applying for a job at Iconsys.

Typical information will include some or all of the following depending on the services we are providing you:

Identification and contact data – Email Address, Name, Phone Number, Postal Address

Enhanced identification data – ID Documents (Driving Licence, Passport, Immigration Status)

Financial Data – bank details, Tax and National Insurance information, credit card information and who is paying for care

Employment Data – CV, training, reference and qualification information, next of kin

Web Related Data – your IP address, geographical data, cookies

Health Data – Where there is a need to protect you, our clients or other members of staff we may need to collect specific health data

Criminal Records – Where there is a need for us to undertake enhanced verification or legal checks in order for you to work in our sector or for us to undertake specific services on your behalf.

## Collecting Personal Data

When we collect personal data, you will be provided with a Privacy Notice that will detail:

1. Who we are
2. What personal information we are collecting
3. Why we need it
4. Legal Basis under which we are processing (typically 'Consent', 'Contractual Obligations' and/or 'Legitimate Interest') (<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/>)
5. What we are going to use it for and any decisions (automated or human) that it will be used for
6. Who that information will be shared with
7. The safeguards we have put in place to protect your information
8. Our standard retention period or legal need to retain that information
9. Your rights <https://www.iconsys.co.uk/uploads/2020/06/Your-Rights-privacy-notice-updated-10th-May-2018.pdf>

Some of the information we collect is provided here:

- Personal Identification Data – Name, Address, Passport, Immigration Status, Banking Information.
- Sensitive Personal Data – Health/Medical/Wellbeing, Religious, Racial.
- Legal Status – your legal status in respect of the services we are undertaking for you, and/or the status of those that can act on your behalf.

## How we collect Personal Data

Depending on the nature of our engagement we may collect personal data in a variety of ways.

- We may collect this information directly from you
- We may collect this information from your relative
- We may collect this information from a Health Care Professional in the event that you come to us via a Health Provider (such as the NHS or Social Services).

## What we use that Personal Data for

The specific use of Personal Data will be detailed in the relevant Privacy Policy for the specific service(s) we are providing you.

As a general guide we use Personal Data to:

1. Deliver the services that we have contracted with you to provide. In these circumstances the legal basis of processing is likely to be Contractual Obligation which will be detailed in the relevant Privacy Policy for that service. Depending on how you have asked us to communicate with you e.g. Phone, Text Message, Email, or how we are required to communicate with you e.g. secure Royal Mail deliveries we will use one or many of the methods you have provided us with. In some cases, we may be required by law or for security reasons to communicate with you in a specific manner. This will be made clear in the relevant Privacy Policy.
2. Process information relating to Job Applications. In these circumstances we will use your information for the purpose of screening and selection against criteria for roles within our organisation. Depending on the role we may undertake further screening of your information with third-parties for example to undertake DBS, Criminal Records as well as medical/health checks in order to protect you and our clients. You will be informed of this as part of our recruitment process. Nothing will be shared with a third party without your consent. As an employer we may also be required to provide statistical information as required by employment or industry legislation such as ethnicity, gender etc.
3. Populate our Marketing Database. If you are an existing customer or have enquired about a product we will send you news about relevant products and services based on your preferences at the time unless you have opted-out of receiving contact from us. You will be asked about this at the time of engagement.
4. Web site Cookies. We use web site cookies to enhance your experience when visiting our site. For a period of time, defined by the Internet Service Providers retention policy, your IP address can be used to identify you (or your location) and as such constitutes personal data. We do not explicitly use this information ourselves, but we do use it to monitor where visitors are coming from and what is being looked at on our site. If you choose not to use cookies or you prevent their use through your browser settings, you will not be able to use all the functionality of our website.

We use cookies in the following ways:

- 1.1. to track how you use our website
- 1.2. to record whether you have seen specific messages we display on our website

This list is not exhaustive but designed to provide you indicative uses of your personal data. Please ensure you read the appropriate Privacy Policy for the product or service we are providing you for specific information.

## Links to other sites

We may provide, from time to time, links to our blog articles or other web links.

Because we have no control over these sites, we cannot take responsibility for the practise they may undertake in respect of privacy and/or protecting your Personal Data. We would therefore advise you to satisfy yourselves that these sites are operating privacy policies that inform you how they handle and protect your data – as we cannot take any responsibility for this.

### Social Media Widgets and Links

You are probably familiar with social media which contain “Like” buttons and the various “Share” buttons that are available to users of the internet.

Social Media service providers may collect Personal Data about you, such as IP address, pages you visit on our site and may set their own cookies to enable them to function properly. In much the same way as *Links to other sites* do not allow us to enforce our policies, we would suggest that you undertake the same checks regarding the privacy policy of the company providing those features.

### Third Parties – Service Providers, Business Partners and others

We work with several third-party services providers who undertake services for us, these include:

Service Provider or Provider Type	Service Provided to us or you
GP, Medical Assessment, Occupational Health	Potentially to assess your ability to work for us and to ensure we can meet your needs. In the case of you being a resident, this will be necessary to ensure that we can meet your needs initially and on an ongoing basis. This is on the basis of protecting your vital interests as well as those of our staff and clients.
Health Care providers in the event of an emergency	To ensure that in the event you become unwell we are able to provide the necessary information to assist with you receiving the necessary medical attention. This is to protect your vital interests.
Your previous employer or references	Provision of feedback on your previous roles or you as an individual, this on the basis of our legitimate interests.
Professional Bodies and Certification Boards	To ensure that you have the necessary professional certifications required for us to employ you and for any ongoing sector specific requirements of professional competence. This on the basis of our legitimate interests.
Health and Life Insurance bodies	In the event that you travel on business and/or are entitled to private medical or life insurance we are required to pass on certain information to the companies that provide these services on

	our behalf. This is on the basis of our contractual obligations with you.
--	---

In most cases you will be made aware of the parties that we share information with, prior to us sharing this information.

### **Where we may share your information without your explicit consent**

We may be required or chose to share your information in certain circumstances without obtaining your explicit consent, some examples of this would be:

- To comply with any legal process, applicable law or governmental request e.g. warrant, subpoena, statutory reporting, sector specific compliance
- To enforce/administer our agreements
- To protect our company or the public from harm or illegal activities
- For fraud prevention, investigation, risk assessment
- To protect the rights and property of our company
- To defend ourselves against third-party claims or allegations

In any event, we will consider your rights and privileges before sharing this information.

### **How you can help protect your Personal Data**

In all cases, the information we require to obtain for you is necessary in the provision or assessment of the provision of services to you. We rely on this information being accurate and up to date, which is in part our responsibility as well as yours.

However, in many cases you are able to limit the use of your information for services that do not require your data. However, limiting your information may result in you not being able to receive that optional service.

#### Changes to your Personal Data

In the event that your Personal Data, that we use to provide you goods or services, changes e.g. your surname, address, email address or Sensitive Personal Data E.g. Religion, Health Data – it is critical that you inform us of these changes to ensure we have the correct information on our systems. Where you have access to administer these changes yourself we would expect you, if you are able, to update these details accordingly or else inform us of changes as soon as possible.

#### Mailing List Opt-In – Marketing Emails

You may opt-out of receiving marketing emails and newsletters from us by using the unsubscribe link within each email or contacting us directly.

Opting out of marketing lists, only removes you from such communication. Transactional emails e.g. those relating to services we are providing to you or responding to queries or enquires you make to us, may still result in us emailing you information where that medium is most appropriate.

### **Security**

Iconsys operates against a Privacy by Design and By Default policy. This means that before we use your data we have already considered the potential impact on you were your data to be lost, stolen, shared or compromised.

We undertake routine reviews of our processes and security policies in order to ensure that we can take all reasonable precautions in protecting your data.

Where at all possible we encrypt all information that is either stored or transmitted to third-parties. Where data is stored or transmitted to a Third Country (any country outside of the European Economic Area (EEA)) we will ensure appropriate adequacy protection is in place in accordance with Data Protection Legislation.

Consequently, we may also need to sometimes undertake further security and screening questions when undertaking our routine dealings with you these are there to protect your personal data and security.

Whilst we undertake all reasonable precautions, encryption, software updates and patches, we cannot guarantee the safety of data transmitted over the internet.

### **Data Breach**

In the event of a Data Breach of your Personal Data, which means:

“The unintended loss, destruction amendment or disclosure of Personal Data”

We will first do all that is necessary in order to minimise the impact on you, identify any potential malicious third-party, identify any third-parties that may also be impacted and take all reasonable efforts to ensure that you are notified.

In the event that we are notified by a third-party of a breach, in their systems, we will undertake the same level of efforts.

We will undertake this communication either directly with you as an individual or by sending out a public notification.

At the same time, we will comply with the current law in respect of informing the appropriate Supervisory Authority which is currently the Information Commissioners Office (ICO). We are under a legal requirement to report Data Breaches to the ICO.