Data Protection & Privacy Policy
May 2018

Version 1

IRS (Northern) Ltd

26 Strickland Street, Hull, HU3 4AQ

Tel: 01482213308
Email: info@irsn.co.uk

SP04

Data protection & Privacy Policy

On the 25th May 2018, processing of personal data by organisations will have to comply with the General Data Protection Regulation (GDPR)

Our Privacy Promise

We Promise:

1: To keep your data safe and
2: Not to sell your data
3: To give you ways to manage and review your marketing choices at any time

How your personal information is used by IRS (Northern) Ltd.

Your information will be held by IRS (Northern) Ltd. More information on our company can be found at www.irsn.co.uk

1. Introduction

We at IRS (Northern) Ltd respect your right to privacy and comply with our obligations under the latest General Data Protection Regulation, (GDPR).

The purpose of this document is to explain how we deal with any personal data you provide to us while visiting our website, emailing us or contacting us by telephone. Naturally, if you are not happy with this Privacy policy, you should not use this website. Any external links to other websites are clearly identifiable as such, and we are not responsible for the content or the privacy policies of these other websites.

2. Who are we?

IRS (Northern) LTD is a company that provides both new manufactured and used refrigeration units. We also install and safely remove refrigeration units along side of servicing. If you have any questions, or want more details about how we use your personal information, you can ask us by sending an email to; info@irsn.co.uk

Or by calling our office on 01482 213308, or writing to us;
IRS (Northern) Ltd
26 Strickland Street
Hull
HU3 4AQ

For the Data Protection Act 1998, Data Protection Bill when in force and all other relevant legislation, Mr Alex Moore, Director of IRS (Northern) Ltd is the "**Data Controller**" and is responsible for the controlling of your personal data. We welcome any feedback or questions you may have.

If at any time you wish for your data to be deleted from our records, or wish to know what data we hold on you, then please contact our data controller by email at alex@irsn.co.uk

3. Types of Information Collected

We retain two types of information:

Non-Personal Data

Like most other websites, we gather statistical and other analytical information collected on an aggregate basis of all visitors to our website. This Non-Personal Data comprises information that cannot be used to identify or contact you, such as demographic information regarding, for example, user IP addresses where they have been clipped or anonymised, browser types and other anonymous statistical data involving the use of our website, IRS (Northern) Ltd uses Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics use cookies to help how we analyse how visitors to our website use our website. View Google Analytics

Personal Data
This is data that identifies you or can be used to identify or contact you and is submitted by you voluntarily through an enquiry form on our website and will include;

- **Your name** This is collected to allow us to address you
- **Your email address** This is collected to allow us to reply to your enquiry
- **Your contact telephone number** This is collected so that we can quote for our services
- **Your Post Code** This is collected so that we can quote for the delivery of materials
- **The name of your company if applicable** This is collected to that we can visit your website and understand your business.
- **The nature of your enquiry** This is collected to allow us to have a clearer initial understanding of what type of air conditioning system you require and the nature of your enquiry.

Privacy Policy

The information generated by the cookie about your use of our website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of our website, compiling reports on website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. We use information to keep our site relevant and to make it easier to use.

We do not and will not collect details of a person's;

- Age
- Race
- Ethnic origin
- Political preferences
- Religion
- Trade union membership
- Health
- Sexual orientation

4. Other Personal Information we use

Maintaining historical records

We use an electronic folder system for each enquirer, each with a unique enquiry number which is stored on our server with an encrypted back up in the cloud.

1) If after 24 months a potential customer has not purchased anything from us, then we permanently delete their data from the folder system.
2) If a customer does purchase from us or use our services, then we retain their information on our server and in the cloud. We retain the information for communication purposes only and being able to contact the customer over any potential warranty issues.
3) Any orders issued to suppliers or invoices to customer are kept in the event that they are required by the Inland Revenue/VAT department in the future.

We do not retain any financial information on our server or in the cloud with regards to any bank account detail of our customers

Credit Card Payments
We do not accept credit card payments.

Bank Details Retained
We retain our suppliers company name, bank account number and sort code so that we can make payments to them in the future. This information is stored on a secure HSBC business website.

Email Marketing
We don't not undertake email marketing.

5. Protection of Data we keep

All data we manage is kept on our server which has an encrypted back up to the cloud. No personal information is kept on any employee's laptop/desktop computer. When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

6. Disclosure of Information to Third Parties

We will not disclose your Personal Data to any third parties. We will disclose your Personal Data if we believe in good faith that we are required to disclose it in order to comply with any applicable law, a summons, a search warrant, a court or regulatory order, or other statutory requirement.

7. Website & Cookie Privacy Policy

We value your privacy and will take all appropriate steps to protect it. Our policy has been very simply written but is comprehensive in protecting you and your preferences. This policy clearly outlines what data we collect, how it is used, how you can give and withdraw consent and how you can have your data amended/erased.
We collect information from and about you in three ways; directly – via forms you fill in or via messages/emails sent via the website and indirectly – via the use of cookies – via a telephone enquiry.

What are cookies?
A cookie is a text-only string of information that a website transfer to the cookie file of the browser on your computer or mobile devices so that the website can remember who you are. A cookie will typically contact the name of the domain from which the cookie has come, the 'lifetime' of the cookie, and a value, usually a randomly generated unique number. Cookies can help a website to arrange content to match your preferred interests more quickly and are used by most major websites. Cookies cannot be used by themselves to identify you.

8. Security

The nature of the Internet is such that we cannot guarantee or warrant the security of any information you transmit to us via the Internet. No data transmission over the internet can be guaranteed to be 100% secure. However, we will take all reasonable steps (including appropriate technical and organisational measures) to protect your Personal Data.

9. Data Protection Supervisory Authority

The Data Protection Supervisory Authority in the UK is the Information Commissioners Office. Should you have any complaints about the way we handle your data, you may direct them to the ICO. More information on the ICO can be found on their website www.ico.org.uk/

10. Changes to the Website Privacy Policy

Any changes to this Website Privacy Policy will be posted on this website so you are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If at any time we decide to use Personal Data in a manner significantly different from that stated in this Website Privacy Policy, or otherwise disclosed to you at the time it was collected, we will update this privacy policy.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **will not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **IRS (Northern) Ltd will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data accuracy

The law requires IRS (Northern) Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort IRS (Northern) Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.

- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- IRS (Northern) Ltd will make it **easy for data subjects to update the information** IRS (Northern) Ltd holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by IRS (Northern) Ltd are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, IRS (Northern) Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

IRS (Northern) Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

The Administrator will on behalf of the Managing Director will periodically review and communicate the Policy to all employees and will identify responsibilities for the management and ensure adequate resources are available to implement the Policy.

Signature 

Name **ALEX MOORE**
Position **Director**
Date **02/05/2018**