



SAFETYNET SOLUTIONS

SAFETYNET SOLUTIONS & THE GENERAL DATA PROTECTION REGULATION

GDPR 25.05.18

DISCLAIMER:

Please note this information is provided as a SafetyNet Solutions Guideline,

It is not intended to be a legal document and does not constitute legal advice.

Safetynet Solutions Ltd cannot accept any liability whatsoever arising from any interpretation of the contents of this document and all readers are advised to seek their own legal counsel.

Data Controller means the person who determines the purposes and means of processing Personal Data

Data Processor means a person which processes Personal Data on behalf of a Data Controller

Data Protection Legislation means the United Kingdom's Data Protection Act 1998 and from 25 May 2018 the General Data Protection Regulation and any legislation implemented in connection with the General Data Protection Regulation and any replacement legislation coming into effect from time to time including (without limitation) any replacement legislation implemented by the United Kingdom following the withdrawal of the United Kingdom from the European Union

Data Transfer Agreement means a data transfer agreement entered into by the parties on the terms approved by the European Commission in Decision 2010/87/EU

General Data Protection Regulation means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

Personal Data means information relating to an identifiable natural person.

Data Protection Requirements for UK Data

CLAUSE X

XA.1 The parties acknowledge that during the term of this Agreement in connection with the provision of the Services the Vendor is required to process Personal Data on behalf of the client. In order to ensure that the Client is able to comply with the Data Protection Legislation, the Vendor agrees to comply with the obligations set out in this Section XA in relation to the processing of Personal Data. A description of the Personal Data and the processing activities undertaken by the Vendor is set out in the table below. The rights and obligations of the Client in connection with the data processing activities are set out in this clause XA and the other terms of this Agreement. If any of the provisions in this clause XA conflict with any of the other provisions of this Agreement, the provisions set out in this clause XA shall prevail.

Categories of data

Contact details, employment data and information about goods and services provided

Categories of data subjects

Customers, potential customers and employees, visitors and contractors



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk
sales@safetynetsolutions.co.uk

Processing Operations

Storing, data entry, amending and transmitting of data relating to visits to the client's premises

Location of Processing Operations

Manchester, UK

Identity of sub-contractors

UKFast

Purposes

ISP and Secure Cloud Hosting centre to provide services for visitor management.

Duration

Relevant data may be retained during the term of the Agreement and deleted upon the termination of the Agreement.

XA.2 To the extent that the Vendor processes Personal Data on behalf of the Client in connection with this Agreement, the Vendor shall:

XA.2.1 solely process the Personal Data for the purposes of fulfilling its obligations under this Agreement and in compliance with the Client's written instructions as set out in this Agreement and as may be specified from time to time in writing by the Client;

X.A.2.2 notify the Client immediately if any instructions of the Client relating to the processing of Personal Data are unlawful;

XA.2.3 not transfer to or access any Personal Data from a country outside the European Economic Area and following the withdrawal of the United Kingdom from the European Union, the United Kingdom, without the prior written consent of the Client;

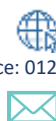
XA.2.4 comply with the Client's instructions in relation to transfers of Personal Data to a country outside the European Economic Area or following the withdrawal of the United Kingdom from the European Union, the United Kingdom, unless the Vendor is required pursuant to Applicable Laws to transfer Personal Data outside the European Economic Area, or following the withdrawal of the United Kingdom from the European Union, the United Kingdom, in which case the Vendor shall inform the Client in writing of the relevant legal requirement before any such transfer occurs unless the relevant law prohibits such notification on important grounds of public interest;



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk



XA.2.5 not engage any sub-contractor to carry out any processing of Personal Data without the prior written consent of the Client, provided that notwithstanding any such consent the Vendor shall remain liable for compliance with all the requirements under this Agreement;

XA.2.6 ensure that obligations equivalent to the obligations set out in this Section are included in all contracts between the Vendor and permitted subcontractors who will be processing Personal Data;

XA.2.7 take appropriate technical and organisational measures against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data taking into account the harm that might result from such unauthorised or unlawful processing, loss, destruction or damage and the nature of the Personal Data to be protected;

XA.2.8 taking into account the nature of the data processing activities undertaken by the Vendor provide all possible assistance and co-operation (including without limitation putting in place appropriate technical and organisations measures) as requested by the Client from time to time to enable the Client to fulfil its obligations to respond to requests from individuals exercising their rights under the Data Protection Legislation;

XA.2.9 provide assistance as requested by the Client from time to time to ensure compliance with the obligations set out in Articles 32 to 36 (inclusive) of the General Data Protection Regulation taking into account the nature of the data processing undertaken by the Vendor and the information available to the Vendor; and

XA.2.10 notify the Client immediately in writing if:

XA.2.10.1 the Vendor or any sub-contractor engaged by on behalf of the Vendor suffers a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data; or

XA.2.10.2 the Vendor or any sub-contractor engaged by on behalf of the Vendor receives any data security breach notification, complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation, and in each case the Vendor shall provide full co-operation, information and assistance to the Client in relation to any such data security breach, complaint, notice or communication;

XA.2.11 upon termination of this Agreement, at the choice of the Client, delete securely or return all Personal Data to the Client and delete all existing copies of the Personal Data; and

XA.2.12 make available to the Client all information necessary to demonstrate compliance with the obligations set out in this Section XA and allow for and contribute to audits, including

inspections, conducted by or on behalf of the Client or by a data protection supervisory authority (including the United Kingdom's Information Commissioner).

XA.3 The Parties acknowledge that:

XA.3.1 the deadline for implementation of the General Data Protection Regulation will occur during the term of this Agreement;

XA.3.2 as at the date of this Agreement legislation relating to certain aspects of the General Data Protection Regulation has not been implemented;

XA.3.3 the regulators have not issued guidance in relation to their requirements in relation to the General Data Protection Regulation; and

XA.3.4 the United Kingdom may leave the European Union during the term of this Agreement, which may result in changes to the Data Protection Legislation.

XA.4 In light of the factors set out in Section XA.3, the Parties agree that if there are changes to the Data Protection Legislation or related guidance from regulators during the term of this Agreement which require either Party to take additional steps to enable compliance with their regulatory obligations, the Parties shall review the provisions in this Agreement and shall negotiate in good faith to agree changes to this Agreement to enable compliance with updated Data Protection Legislation or related guidance from any regulators. If the parties cannot agree changes to the Agreement to give effect to the requirements of updated Data Protection Legislation by 25 May 2018 to the reasonable satisfaction of the Client, the Client shall be entitled to terminate the provision of the Services to the UK branches of the Client with immediate effect by giving written notice to the Vendor."

Signed:



Name: Lisa Alderson-Scott

Position: Director

Date: 3rd May 2018



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk

SAFETYNET SOLUTIONS LTD. PRIVACY NOTICE

1. INTRODUCTION

This privacy notice provides you with details of how we collect and process your personal data with regards to collection within Safetynet, and processing for SkyVisitor (and other Safetynet software).

Safetynet Solutions Ltd is the data controller and we are responsible for your personal data (referred to as “we”, “us” or “our” in this privacy notice) only where this directly collected by Safetynet as a company entity or by any employee.

Where the data is collected via SkyVisitor (or El Vis.net) we are the Data Processor and our client is the Data Controller.

Our email address is **office@safetynetsolutions.co.uk**

Our postal address is **Safetynet Solutions Ltd. Lancaster House, Lancaster Fields, Cheshire CW1 6FF**

If you are not happy with any aspect of how we collect and use your data, you have the right to complain to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We should be grateful if you would contact us first if you do have a complaint so that we can try to resolve it for you.

If you have a query with regards to your data collected via SkyVisitor, this should be referred to the SkyVisitor site.

It is very important that the information we hold about you is accurate and up to date. Please let us know if at any time your personal information changes by emailing us at gdpr@safetynetsolutions.co.uk

Sensitive Data

5

We do not collect any Sensitive Data about you as a client. Sensitive data refers to data that includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data. We do not collect any information about criminal convictions and offences.

Where the data is collected via SkyVisitor (or El Vis.net) we are the Data Processor and our client is the Data Controller.

Should our client need to collect the following sensitive data about you in order to comply with Health & Safety Legislation, risk assessment and duty of care, this may include data with regards to your health and mobility, illnesses and any special needs.

SkyVisitor will enable them to make you explicitly aware that they have grounds for processing sensitive data and we will request your active acknowledgement of this consent.

2. HOW WE USE YOUR PERSONAL DATA

We will only use your personal data when legally permitted. The most common uses of your personal data are:

Where we need to perform the contract between us.

- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Generally, we do not rely on consent as a legal ground for processing your personal data, other than in relation to sending marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by

Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk




www.safetynetsolutions.co.uk
Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk

emailing us at gdpr@safetynetsolutions.co.uk

Purposes for processing your personal data

Set out below is a description of the ways we intend to use your personal data and the legal grounds on which we will process such data. We have also explained what our legitimate interests are where relevant.

We may process your personal data for more than one lawful ground, depending on the specific purpose for which we are using your data. Please email us at gdpr@safetynetsolutions.co.uk if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests to recover debts owed to us
To process your Visitor data collected via SKYVISITOR 	(a) Identity (b) Contact (c) Possibly sensitive (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for to comply with a legal obligation (c) Necessary for your legitimate interests to keep your records updated and study your footfall on site.
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests to keep our records updated and to study how customers use our products/services



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics

 www.safetynetsolutions.co.uk
 Service: 01270 508 565 / Sales: 01270 508 550
 sales@safetynetsolutions.co.uk



To enable you to partake in a prize draw, competition or complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests to study how customers use our products/services, to develop them and grow our business
To administer and protect our business and our site (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise (b) Necessary to comply with a legal obligation
To deliver relevant content and advertisements to you and measure and understand the effectiveness of our advertising	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests to define types of customers for our products and services, to keep our site updated and relevant, to develop our business and to inform our marketing strategy
To make suggestions and recommendations to you about goods	(a) Identity	Necessary for our legitimate interests to develop our products/services and grow our business

or services that may be of interest to you	(b) Contact (c) Technical (d) Usage (e) Profile	
--	--	--

Marketing communications

You will receive marketing communications from us if you have:

- (i) requested information from us or purchased goods or services from us; or
- (ii) if you provided us with your details and ticked the box at the point of entry of your details for us to send you marketing communications; and
- (iii) in each case, you have not opted out of receiving that marketing.

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

You can ask us or third parties to stop sending you marketing messages at any time by emailing us at gdpr@safetynetsolutions.co.uk at any time.

Where you opt out of receiving our marketing communications, this will not apply to personal data provided to us as a result of a product/service purchase, warranty registration, product/service experience or other transactions.

3. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share your personal data with the parties set out below for the purposes set out in the table in paragraph 2 above:

Service providers who provide IT and system administration services.

- Professional advisers including lawyers, Clienters, auditors and insurers who provide consultancy, Clienting, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities based in the United Kingdom and other relevant jurisdictions who require reporting of processing activities in certain circumstances.
- Third parties to whom we sell, transfer, or merge parts of our business or our assets.

We require all third parties to whom we transfer your data to respect the security of your personal data and to treat it in accordance with the law. We only allow such third parties to process your personal data for specified purposes and in accordance with our instructions.

6. INTERNATIONAL TRANSFERS



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk

With regards to where we are Data Processors for **SkyVisitor**, we do not transfer your personal data outside the European Economic Area.

For our direct business customers, we may transfer your personal data outside of the EEA for utilisation with specific marketing tools, such as Mailchimp. Whenever we transfer your personal data out of the EEA, we do our best to ensure a similar degree of security of data by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission; or
- Where we use certain service providers, we may use specific contracts or codes of conduct or certification mechanisms approved by the European Commission which give personal data the same protection it has in Europe; or
- Where we use providers based in the United States, we may transfer data to them if they are part of the EU-US Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US.

If none of the above safeguards is available, we may request your explicit consent to the specific transfer. You will have the right to withdraw this consent at any time.

Please email us at gdpr@safetynetsolutions.co.uk if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

7. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know such data. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax purposes.

In some circumstances you can ask us to delete your data: see below for further information.

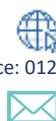
In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk
Sales: 01270 508 550
sales@safetynetsolutions.co.uk

9. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data. These include the right to:

- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to processing of your personal data.
- Request restriction of processing your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.

You can see more about these rights at:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

If you wish to exercise any of the rights set out above, please email us at gdpr@safetynetsolutions.co.uk

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

We assume that the user of our applications has taken notice of this Privacy Statement. Be aware that we do occasionally update this Privacy Statement, and that it is your responsibility to examine and take notification of any change made to this document. So please do return and review this Statement on a regular basis. Any substantial change will be clearly communicated.



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk

Data Controller? Or Data Processor?

Safetynet is only the Data Controller for the processing of personal data for Safetynet's direct business purposes. This means the processing of personal data of our clients' in relation to their business needs (sales, marketing, service, accounts).

If you are a user of SkyVisitor or El Vis.net, or if you are a visitor of one of SkyVisitor locations, it is the person(s) responsible at the location who identifies as the 'Data Controller'. Safetynet Solutions Ltd. is acting as the customer's "data processor". In such case, our customer is the one assuming responsibility for the processing of personal data through our services.

SkyVisitor and El Vis.net data is held securely under ISO27001 via our UK based ISP.



Safetynet Solutions Ltd is Cyber Essentials certified.

Safetynet Solutions Ltd adheres to the Data Protection Principles in its business practices and deploys configuration options in the SkyVisitor application to enable the client Data Controller to adhere to the same, in line with their own Privacy Notice.



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



www.safetynetsolutions.co.uk
Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



Data Protection Principles:

LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

DATA MINIMISATION

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

12

ACCURACY

Personal data shall be accurate and, where necessary, kept up to date.

STORAGE LIMITATION

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed Integrity and confidentiality Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

INTEGRITY AND CONFIDENTIALITY

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk



WHAT ARE YOUR LAWFUL GROUNDS FOR PROCESSING?

In the management and Identification of Visitors and Staff on site, we understand that your lawful grounds for processing fall mainly into point 3 below, with regards to compliance with Health and Safety legislation; with point 4 the same, in line with your duty of care over their safety and well-being; and with point 2 in line with any contractual obligation you may have with any tenant:

1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. Processing is necessary for compliance with a legal obligation to which the controller is subject;
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.



IMAGE
DATA INTELLIGENCE
HEALTH & SAFETY
SECURITY



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics

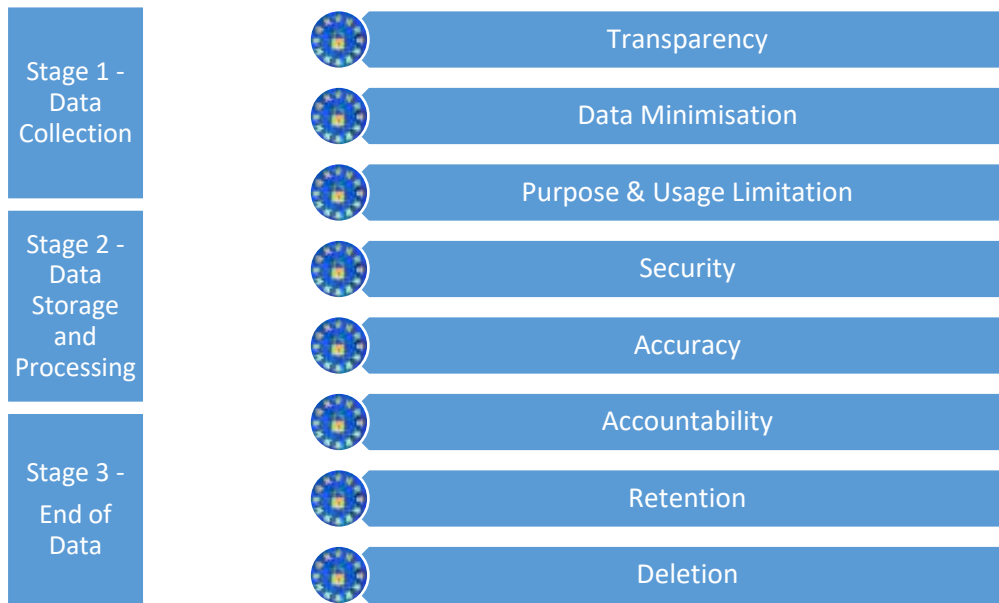


Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk

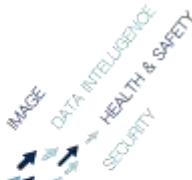




So, in a Nutshell ...

You need to make sure that your 'Data Subjects' *[anyone with Personal Data captured]* are aware that:

- you are capturing the data;
[they are giving the data as you capture it – it is an interaction, you are not collecting it covertly]
- you are only capturing the data you really need for a legitimate purpose
[health & safety obligations, site security]
- you only use it for that purpose
[that it is not transferred onto any mailing list, nor sold to 3rd parties...]
- the data is secured and you know where it is
[secure cloud server – UK data encrypted, secured locally at User level with passwords and Antivirus / Internet Security .. also that it isn't unnecessarily disclosed to others]
- all Data Processors are 'accountable'
[that means 'you', 'us', your reception teams, your security staff – your users who type it in]
- you only keep as long as necessary
[... how long is necessary? .. a civil claim can be made up to 3yrs from incident, some health and safety records need to be kept for 40 years So, we will make the option to remove the data 'a granular'- decision i.e.. at 'field' level, rather than the entire record...and variable per visitor type].
- Data is deleted when not required or when legitimately requested for removal
[We will ask you for your Data Purging Policy – additionally, your Data Controllers can also be given permission to delete records]



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk

“Personal Data” as defined by the GDPR

Let's start with how the new laws look at “personal data.” Personal data is anything that contains:

- Directly identifying information such as a person's name, surname, phone numbers, etc.
- Pseudonymous data or non-directly identifying information, which does not allow the direct identification of users but allows the singling out of individual behaviours (for instance to serve the right ad to the right user at the right moment).

The GDPR establishes a clear distinction between directly identifying information and pseudonymous data. The GDPR encourages the use of pseudonymous information and expressly provides that “the application of pseudonymising to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations”.

“Sensitive Data” as defined by the GDPR.

Sensitive data is any data that reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health or a natural person's sex life and/or sexual orientation



SkyVisitor Data Controllers will be able to set their process for handling, retaining and removing Personal Data and Sensitive Data at a granular field level on a daily control setting.



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk
sales@safetynetsolutions.co.uk

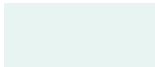
Data Classification Examples:



Personal Data-Key Identifier



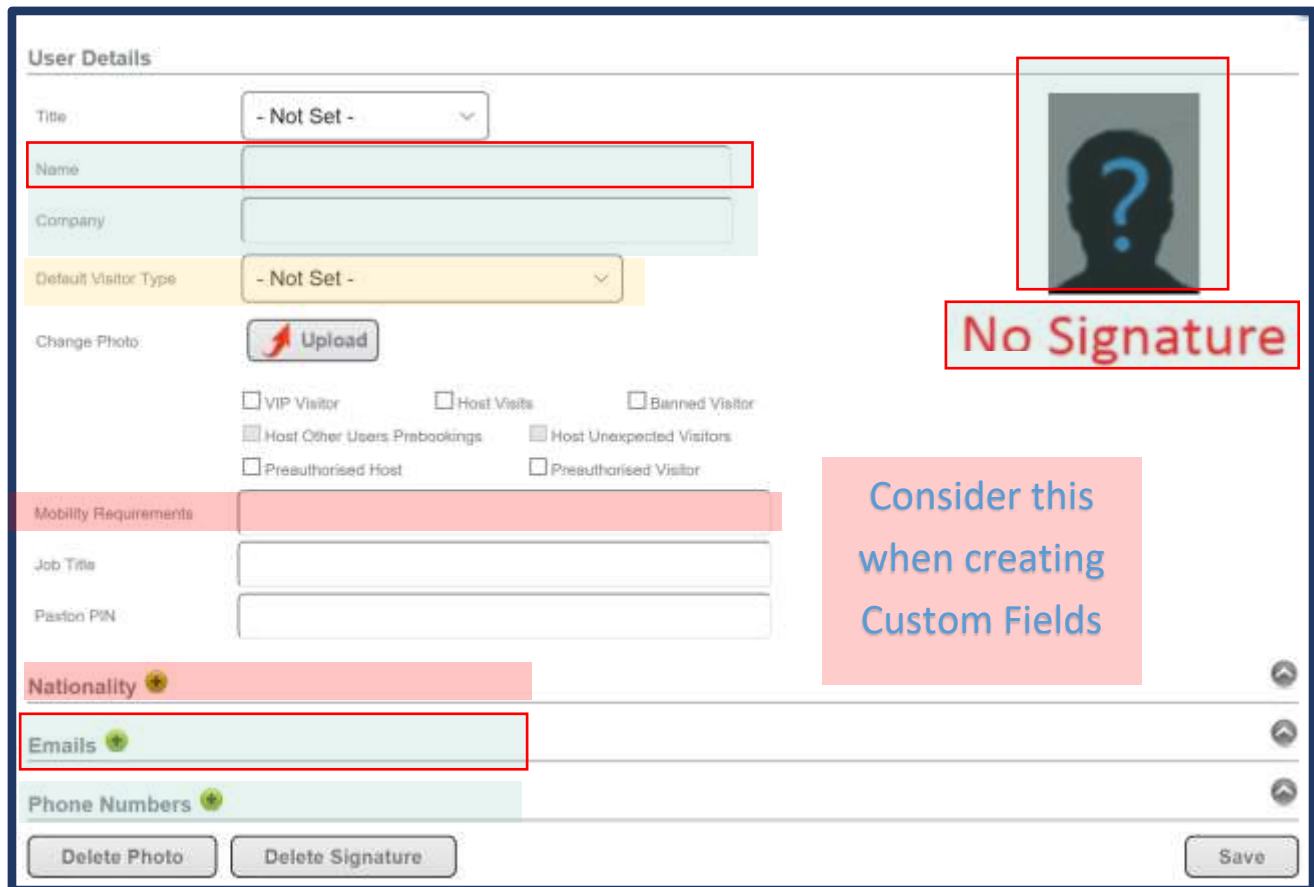
Sensitive Data



Not Personal Data – but may identify when linked or when appears together with a Key Identifier



NOT Personal Data



The screenshot shows the 'User Details' form in SkyVisitor. Various fields are highlighted with colored boxes to illustrate data classification:

- Personal Data-Key Identifier (Light Blue):** Name, Company, Email.
- Sensitive Data (Pink):** Mobility Requirements, Nationality.
- NOT Personal Data (Yellow):** Default Visitor Type.
- Not Personal Data – but may identify when linked or when appears together with a Key Identifier (Light Blue):** Job Title, Pastion PIN.

Other elements in the form include:

- Title: - Not Set -
- Change Photo: Upload button
- Checkboxes: VIP Visitor, Host Visits, Banned Visitor, Host Other Users Prebookings, Host Unexpected Visitors, Preauthorised Host, Preauthorised Visitor.
- Nationality: + icon
- Emails: + icon
- Phone Numbers: + icon
- Buttons: Delete Photo, Delete Signature, Save.
- Placeholder: A box with a question mark icon and the text 'No Signature'.
- Annotation: A pink box with the text 'Consider this when creating Custom Fields'.

16

PARTIES

[1] Data CONTROLLERS - Our SkyVisitor Clients & [2] Data PROCESSORS - Safetynet Solutions Ltd

also in place with our Data Processors, where we are the Data Controller (i.e. our relevant subcontractors and 3rd party suppliers).

BACKGROUND:

(A) The Controller and the Processor entered into a SkyVisitor SAAS contract **UNDER WHICH THE PROCESSOR IS PROVIDING THE VISITOR MANAGEMENT SYSTEM CLOUD SERVICE** that requires the Processor to process Personal Data on behalf of the Controller.

(B) This Processor Agreement (**Agreement**) sets out the terms and conditions on which the Processor will process Personal Data when providing services under the Services Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

AGREED TERMS:

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Data Protection Legislation: all applicable data protection laws including GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

Data Subject: an individual who is the subject of Personal Data.

GDPR: General Data Protection Regulation ((EU) 2016/679).

Personal Data: means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.2 The Schedules form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.3 A reference to writing or written includes email.

2. PROCESSING PURPOSES

2.1 The Controller and the Processor acknowledge that the Controller is the controller and the Processor is the processor and that the Controller retains control of the Personal Data and remains responsible for its compliance obligations under Data Protection Legislation.

2.2. Where the Processor appoints a subcontractor pursuant to clause 4 below, the Processor shall be a data controller in relation to such processing.

2.3 The Processor may process the Personal Data categories and Data Subject types set out in Schedule 1 of this Agreement.

3. PROCESSOR'S OBLIGATIONS

3.1 The Processor shall:

- 3.1.1 implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of Data Protection Legislation and ensure the protection of the rights of the Data Subject, as further set out below in this Agreement;
- 3.1.2 only use subcontractors to help with the processing of Personal Data in the circumstances set out in clause 4 below;
- 3.1.3 process the Personal Data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- 3.1.4 ensure that persons authorised to process the personal data (such as its employees) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- 3.1.5 take the security measures set out in clause 5 below;
- 3.1.6 taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights as set out in clause 6 below;



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk
Sales: 01270 508 550

- 3.1.7 assist the Controller in ensuring compliance with the obligations set out in clause 7 below (data breach) taking into account the nature of processing and the information available to the Processor;
- 3.1.8 at the choice of the Controller, delete or return all the Personal Data to the Controller after the termination or expiry of the Services Agreement and delete existing copies (unless Union or Member State law requires storage of the Personal Data);
- 3.1.9 make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;
- 3.1.10 assist the Controller in ensuring compliance with the requirement to carry out Data Protection Impact Assessments as set out in Article 35 of GDPR, taking into account the nature of processing and the information available to the Processor;
- 3.1.11 Designate a Data Protection Officer if required by Article 37(1) of GDPR and in accordance with the provisions of Articles 37, 38 and 39 of GDPR; and
- 3.1.12 immediately inform the Controller, if in the opinion of the Processor, an instruction from the Controller infringes Data Protection Legislation.

19

- 3.2 The Processor will promptly comply with any request by or instruction from the Controller to process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.3 The Processor will immediately notify the Controller if in its opinion, the Processor carrying out the processing of Personal Data on an instruction from the Controller would infringe any provision of Data Protection Legislation.
- 3.4 The Processor will keep all Personal Data confidential and not disclose such data to third parties unless specifically authorised in writing by the Controller or as required by law. If the Processor is required by law, court, regulator or supervisory authority to process or disclose any Personal Data, the Processor will first inform the Controller of this and allow the Controller to object or challenge the requirement, unless the law prohibits the Processor from informing the Controller.

4 SUBCONTRACTORS

- 4.1 The Processor may only authorise a third party ("subcontractor") to process the Personal Data if:
 - 4.1.1 the Processor has made this information available to the Controller of each appointment of a subcontractor by means of updating the policy
 - 4.1.2 the Processor has carried out appropriate due diligence on any subcontractor to ensure that the subcontractor can satisfy its contractual obligations; and



IMAGE
DATA INTELLIGENCE
HEALTH & SAFETY
SECURITY



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk

- 4.1.3 the Processor and the subcontractor enter into a written contract containing terms the same as those set out in this Agreement, in particular, in relation to data security measures; and
- 4.1.4 the Processor maintains control over all Personal Data it shares with the subcontractor; and
- 4.1.5 the Processor ensures that the subcontractor does not process the Personal Data except on instructions from the Data Controller (unless required to do so by Union or Member State law); and
- 4.1.6 the contract between the Processor and the subcontractor terminates automatically on termination of this Agreement.

4.2 The Processor shall be fully liable for the actions and inactions of the subcontractor and shall be responsible for the subcontractor's performance of obligations.

5. SECURITY

5.1 The Processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

- 5.1.1 the pseudonymisation and encryption of Personal Data;
- 5.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- 5.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- 5.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

6. RESPONSES TO DATA SUBJECTS

6.1 The Processor will put in place such technical and organisational measures as may be appropriate to enable the Controller to comply with the rights of Data Subjects under Data Protection Legislation, including the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object to processing and the right to object to automated individual decision making.

6.2 If the Processor receives any complaint or other communication relating to the processing of the Personal Data or a Subject

Access Request from a Data Subject, it must notify the Controller as soon as possible after it receives it and in any event within 3 working days and will provide the Controller with all reasonable assistance in helping the Controller to reply to such communications.

6.3 The Processor will provide to the Controller such information as the Controller may reasonably require in order for the Controller to comply with the rights of Data Subjects under Data Protection Legislation. The Processor may not charge an additional amount for fulfilling its obligations under this clause 6.

6.4 The Processor will provide all appropriate assistance to the Controller to enable it to comply with any information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

6.5 The Processor shall not disclose Personal Data to any third party other than at the Controller's written request or as set out in this agreement or as required by law.

7. PERSONAL DATA BREACH

7.1 If any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable ("Personal Data Loss"), the Processor will notify the Controller without undue delay (and in any event within 24 business hours) after learning of such Personal Data Loss and the Processor shall to the extent possible restore any such data at its own expense.

7.2 If the Processor becomes aware of any unauthorised or unlawful processing of the Personal Data or any Personal Data Breach, it will notify the Controller without undue delay (and in any event within 24 business hours) including all relevant information such as:

(a) a description of the nature of the Personal Data Breach, the unauthorised or unlawful processing and/or the Personal Data Loss, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken, or proposed to be taken, including measures to mitigate the impact.

7.3 The parties will co-ordinate and co-operate with each other to investigate any matters arising as contemplated by this clause.

7.4 The Processor shall take all reasonable steps to mitigate the effects and reduce the impact of any Personal Data Breach or unlawful Personal Data processing.

7.5 The Processor agrees that it shall not (and the Controller is solely responsible to):

(a) provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or any other third party, except when the Processor (as opposed to the Controller) is required by law or regulation to provide such notice; and

(b) offer any type of remedy to affected Data Subjects.



8. CROSS-BORDER TRANSFERS OF PERSONAL DATA

8.1 The Processor (or any subcontractor of the Processor) shall not transfer or otherwise process Personal Data outside the European Economic Area (EEA) without obtaining the Controller's prior written consent (except where the Processor is required to transfer such data by Union or Member State law, in which case the Processor shall inform the Controller of such legal requirement before processing takes place, unless any law prohibits such disclosure on important grounds of public interest).

8.2 If the Controller consents to the transfer or other processing of the Personal Data outside of the EEA and no appropriate safeguards exist (such as an adequacy decision or the Processor being part of the EU-US Privacy Shield), the Processor and the Controller will each execute the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Schedule to Commission Decision 2010/87/EU ("SCCs").

8.2 if the Processor appoints subcontractors that are based outside of the EEA, the Processor shall, prior to any Personal Data being transferred to such countries, (i) ensure that such subcontractor executes the SCCs and (ii) send a copy of such executed SCCs to the Controller.

9. TERM AND TERMINATION

9.1 This Agreement will continue for so long as the Processor processes any Personal Data related to the Services Agreement (Term).

10. DATA RETURN AND DESTRUCTION

10.1 The Processor will, on the request of the Controller, provide the Controller with a copy of or access to the Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.

10.2 On termination or expiry of the Services Agreement, the Processor will at least 7 days prior to the date of expiry or termination ask the Controller whether the Controller wants the Personal Data to be deleted, destroyed, returned or retained and shall follow the Controller's instructions accordingly.

10.3 If the Processor is required by any law, regulation, or government or regulatory body to retain any documents or materials, the Processor will inform the Controller in writing of such requirement, providing details of the legal basis for retention and setting out the timings for deletion when such retention period ends.

10.4 If the Controller requires the Processor to delete or destroy certain documents or materials or anything else containing Personal Data, the Processor shall certify in writing that it has so deleted or destroyed the Personal Data within 3 business days of doing so.



12. AUDIT

12.1 The Controller (and any third-party representatives) may audit the Processor's compliance with its obligations under this Agreement and the Processor will give the Controller (and its third-party representatives) all necessary assistance and co-operation to conduct such audits.

12.2 If a Personal Data Breach occurs, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, or if the Controller so requires it, the Processor will:

- (a) conduct its own investigation to confirm the cause of such Personal Data Breach or breach of obligations;
- (b) provide to the Controller a written report on the investigation including any proposals to remedy any problems identified by the investigation; and
- (c) remedy the problems identified within 7 days of the date of the written report.

12.3 On the Controller's written request, the Processor will audit a subcontractor's compliance with its obligations regarding the Controller's Personal Data and provide the Controller with the audit results.

12.4 The Processor will carry out an annual security audit (or at such other periods required by the Controller) identifying any areas of deficiency (when taking into account the scope and nature of the processing of Personal Data and the best practice technologies available at such time) and will provide the written report to the Controller.

23

13. WARRANTIES

The Processor warrants and represents that:

- (a) its employees, subcontractors, agents and any other person or persons processing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;
- (b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and;
- (c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Services Agreement's contracted services.

15. NOTICE

15.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For the Controller: **Client Site**

For the Processor: **Lisa Alderson-Scott** at email gdpr@safetynetsolutions.co.uk

15.2 Clause 15.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable,



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk



any arbitration or other method of dispute resolution.

16. GOVERNING LAW

16.1 This agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance with the law of England and Wales.

16.2 Each party irrevocably agrees that the courts of England and Wales shall have non-exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

Our RECORDS OF PROCESSING shall show:

PERSONAL DATA PROCESSING PURPOSES AND DETAILS:

Subject matter of processing; Duration of Processing; Nature and Purpose of Processing; Data Subject Types; Personal Data Categories.

APPROVED SUBCONTRACTORS:

Name of Sub-Contractor; Location; Contact Details for Person Responsible for Data Protection.

SECURITY MEASURES:

Physical, Virtual, Cyber.



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk



Cyber Security is becoming more important than ever before.

If you want to ensure that your Front of House, or Back of House users are not the weak link in your building's or Occupiers' IT chain you may want to talk further with us....

In partnership with Stonegate IT, we want to offer you the right level of security and protection and have put together a programme to ensure you comply with the National Cyber Security Council Standards.

Choose from Enhanced, Premium or Ultimate and from as little as 50p per day strengthen your Cyber Security with Safetynet & Stonegate.

National Cyber Security Council Standards

	Security	As A	Service
	Enhanced	Premium	Ultimate
Network Security Appliance	✓	✓	✓
Malware Prevention	✓	✓	✓
Removable Media Controls	X	✓	✓
Media Encryption	X	✓	✓
DNS Protection	X	✓	✓
Secure Configuration	✓	✓	✓
User Privileges	✓	X	✓
Security Awareness Training	X	Every 3 months	Every month
Incident Management	X	✓	✓
24 x 7 Monitoring	✓	✓	✓
Secure 2 Factor Authentication	X	X	✓
Security Information and Event Management (SIEM)	ONCE per year	FOUR per year	EIGHT per year
Cyber Essentials Accreditation - Initial	£2295	£2295	£2295
Cyber Essentials Accreditation - Renewal	£1295	£995	£595
Monthly payment per PC from	£15 per PC	£23 per PC	£37 per PC
Installation Fee from	£750	£1100	£1600

25



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics

 www.safetynetsolutions.co.uk
 Service: 01270 508 565 / Sales: 01270 508 550
 sales@safetynetsolutions.co.uk

We would be happy to discuss this further with anyone interested in pursuing enhanced Cyber Security and also to introduce you to our *'Just Add Staff'!* programme which offers a 360° IT equipment supply-data management-security-user training & support option, all the way through to green secure disposal. The full lifecycle of the equipment, data and use.

We offer a *free cyber secure survey* from the outset so that you can see exactly what your vulnerabilities are, and then we can offer you a range of informed solutions with which to secure them.

It's not all about the £ - but when it is, it could be serious ... contact us now to talk further.

Email us at gdpr@safetynetsolutions.co.uk or call us on 01270 508 551 and ask for our *CyberSecure specialists*.

2017 fines.....

- Fines from the Information Commissioner's Office (ICO) against UK companies last year would have been £69m rather than £880,500 if the pending General Data Protection Regulation (GDPR) had been applied, according to industry analysis.
- Fines given to small and medium-sized enterprises could have been catastrophic. For example, [Pharmacy2U's fine](#) of £130,000 would balloon to £4.4m
- GDPR isn't just about financial penalties, but industry analysis is a reminder that there will be significant commercial impacts for organizations that fall foul of the regulations



IMAGE
DATA INTELLIGENCE
HEALTH & SAFETY
SECURITY



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk



sales@safetynetsolutions.co.uk



Safetynet Solutions Ltd confirms that it will be a GDPR compliant organisation no later than 25th May 2018.

GDPR &



SKYVISITOR

Clients who are SkyVisitor Data Controllers will be able to set their process for handling, retaining and removing Personal Data and Sensitive Data at a granular field level on a daily control setting.

Sensitive data will require an 'active' consent for collection.

Personal data is collected for legal and contractual reasons and visitors are made aware.

The data security of SkyVisitor is at ISO27001 level with our ISP.

The data is held in the UK.

*For Data Controller queries relating to Safetynet Solutions Ltd. please contact:
Lisa Alderson-Scott on 01270 508 551 or email gdpr@safetynetsolutions.co.uk.*

For Data Controller queries relating to your data held in SkyVisitor for a site you have attended please contact the site – which is the Data Controller.

Safetynet is acting as a Data Processor in this instance.

Our Data Processor's Agreement is contained herein and is available on request, via email to gdpr@safetynetsolutions.co.uk.



IMAGE
DATA INTELLIGENCE
HEALTH & SAFETY
SECURITY



Head Office: Safetynet Solutions Ltd. Reg GB3903968 Vat Registered Gb 753228239
Lancaster House, Lancaster Fields, Crewe, Cheshire, CW1 6FF
Software Development Centre, Print Manufacturing, Sales, Customer Service & Logistics



Service: 01270 508 565 / Sales: 01270 508 550
sales@safetynetsolutions.co.uk



www.safetynetsolutions.co.uk

