

Group Privacy Notice for website, apps and services

1. Our Role in your privacy

Sign In Solutions (together with its affiliated companies) is committed to ensuring the privacy and confidentiality of your personal information, and to protect it from unauthorised access and disclosure.

The purpose of this Privacy Policy is to clearly communicate to you how we handle your personal information to provide you with services, and to comply with our legal obligations. This Privacy Policy applies to all websites owned or operated by us and our apps and services, as amended from time to time. If you are a customer this Privacy Policy together with our Terms & Conditions of Service (see Annex A), Use of Website Policy and our Data Processing Agreement (see Annex A) will give you a better and more complete understanding of the type of personal information that we hold about you and the way we handle that information.

2. What information will we collect?

Personal data may be collected, stored and used when visiting our website, registering for a trial, or placing an order. The personal information that you are asked to provide, and the reasons why you are asked to provide it, will only be used in ways described in this policy.

Information you provide

- When visiting our website or using our apps.
If you choose to contact us through either of these sources, information you provide such as your name, email address or telephone number and any other information you choose to provide us with will also be stored. If you click a link on our website which redirects you to an affiliates website (or third-party website) you should take the time to read the privacy notice on the affiliates (or third-party) website.
- Account registration.
When registering for an account/trial, details that you provide to us to create a user account and provide you with access to the applications. The registration requires you to provide us with personal contact information, such as your name, company name and email address.
- Payment information.
When paying for your order online, your financial information is directed to our third-party payment processor. We do not store your financial data on our systems (Please see Annex A for any product specific variations).
- Information provided by you so we can provide a service.

This will depend on which service you are using, please see Annex A for product specific variances.

- If you are visiting our premises.
If you are a visitor who has signed into our application, the information provided, such as your name, your company, whom you are visiting and other information that we request, i.e. a photograph or your vehicle registration number (UK).
- Visiting our customer's premises.
If you are signing into our application whilst visiting one of our customers this policy does not apply to you, instead you should defer to their privacy notice. They are acting as the 'Controller' of the data. This means they collect information necessary for the purposes of your visit to their premises. If you want to exercise your rights with the data they hold you should contact them directly.

3. Use of Cookies

We use cookies on our site, you can read more about how we use cookies and how you can change your preferences on our cookies page (see annex A).

4. Purpose of processing

Your data will be processed only for specified, explicit and legitimate purposes. We collect and process the personal data detailed in this policy, and the purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected.

We may, from time to time, use your personal data for reporting and for making improvements to our services; in such instances we will always ensure an individual cannot be identified.

Your personal data may be transferred to our trusted third party processors, this will be for purposes such as: enabling payments, hosting of our servers, project management tools and customer relationship management system.

Our trusted third party processors are contractually bound and have technical, organisational and security measures in place to keep your information confidential and use it only for specified, explicit, and legitimate purposes.

Some messages from us are service-related and necessary for customers. You agree that we can send you non-marketing emails or messages, such as those related to transactions, your account, security, or product changes/updates.

Document Name: Privacy Notice
Document Number: SIS/IG/017
Version: 1
Date of Issue: 01/06/23

If we intend to use any data provided by yourself for marketing purposes, such as sending updates or information relating to the product, we will always make this clear and offer an 'opt out' should you wish not to receive such information.

If you have agreed that we can use your information for marketing purposes, you can change your decision easily, via one of these methods:

- Use the unsubscribe button at the bottom of the email.
- Write to us by email to the appropriate Data Protection Officer for your jurisdiction as specified in section 13.
- Use the "Contact Us" button on our website

We will never lease, distribute or sell your personal data to a third party without requesting your prior permission. We will only transfer your data to other third parties without informing you separately beforehand in the exceptional cases where we are either legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

5. Data quality

If we collect your personal information from our Website, app or whilst providing services to you, we will process it in a way that is adequate, relevant and limited to what is necessary in relation to the purposes for why it is processed. We will maintain and update your information as necessary to keep it accurate or when you advise us that your personal information has changed. We will keep your information in a form which permits your identification for no longer than is necessary. We will hold personal information collected from web enquiry forms for a period of up to 12 months from when the enquiry is closed.

6. Lawful Basis for processing personal data

Our lawful basis for collecting and processing the personal data described in this policy will depend on the type of personal information concerned and the specific context in which we collect it. However, we will generally only collect personal information from you where either;

- We need the personal information to perform our obligations under a contract with you
- The processing is in our legitimate interest and not overridden by your rights
- You have given your consent to do so

We have a legitimate interest in operating our services, for example when responding to your queries, improving our services, or undertaking direct marketing.

If we ask you to provide personal information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not.

7. Security of your data

Protecting personal data from unauthorised access, loss or alteration is of the utmost importance to us. We have physical, technical and organisational procedures to safeguard the information we collect. Our systems are tested annually by an external body to ensure your information is secure. We also conduct internal and external audits so we are confident we comply with the framework standards we have set.

We have put in place appropriate security, privacy and technical 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 on the basis of least-privilege and least-functionality and who have a business need to know. 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. Where will your personal data be processed?

Any transfer of your personal data will follow applicable laws and we will treat the information under the guiding principles of this Privacy Policy.

Sometimes we will need to share your personal data with authorised third parties and suppliers outside your chosen data territory, this will be for purposes such as: enabling payments, project management tools, back office functions and our customer relationship or accounts management system. Your data is shared only when strictly necessary and in accordance with the safeguards and good practices detailed in this privacy policy. Further details of all applicable authorised sub-processors are set out in Annex A.

9. How long will we hold your data?

The length of time we keep your personal data depends on what it is and whether we have an ongoing business need to retain it - for example, to provide you with a service or to comply with applicable legal, tax or accounting requirements.

Data will be retained for as long as your account is active and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with

our data retention policy. Following that period, we'll make sure it's deleted or anonymised.

10. Sign In App use for visitors

If you use Sign In App at our customers premises:

Please note that we are acting as a 'data processor', our customer will be the 'data controller' and will assume responsibility for the processing of personal data and how long that is held for. We have to act upon our customer's instructions regarding data retention. Data will be stored in encrypted backups for 14 days after the retention period in a location selected by the customer.

If you use Sign In App at our premises:

Please note that we are acting as a 'data controller', and will assume responsibility for the processing of personal data for authorised visitors to our premises. Data retention periods will be aligned in accordance with our own data retention policies and local legislation. Data will be stored in encrypted backups for 14 days after the retention period in the EU. Approved visitors who enter our own secured offices are escorted and are required to have their visitor information stored for two years as part of our security measures.

11. Data subject rights

It's your personal data and you have certain rights relating to it. When it comes to marketing communications, you can ask us not to send you these at any time – just follow the unsubscribe instructions contained in the marketing communication, or send your request to unsubscribe@signinsolutions.com please remember to tell us which of our products it's relating to.

You also have rights to:

- know what personal data we hold about you, and to make sure it's correct and up to date
- request a copy of your personal data, or ask us to restrict processing your personal data or delete it
- object to our continued processing of your personal data

You can exercise these rights at any time by sending an email to privacy@signinsolutions.com or your jurisdiction specific DPO.

Document Name: Privacy Notice
Document Number: SIS/IG/017
Version: 1
Date of Issue: 01/06/23

12. Contact Information

As we are a global company with different products, we have data protection officers and privacy officers covering jurisdictions in which they specialise.

- **UK, EU, EEA**
Nicola Petts
Data Protection Officer (UK & EU)
Telephone: Tel: 44 1604 349759
Email: dpo@signinsolutions.com

- **USA, Canada and Global Regions**
Jason Mordeno
Global Privacy Officer
Email: privacy@signinsolutions.com

13. Policy Review Statement

This policy may be reviewed at any time and at the request of either staff or management, but will automatically be reviewed 1 year from the initial approval and thereafter on an annual basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

Document Name: Privacy Notice
Document Number: SIS/IG/017
Version: 1
Date of Issue: 01/06/23

Annex A - Product Specific Disclosures

Applicable legislations in the following regions of USA, Canada, United Kingdom, European Union, European Economic Area and any local laws or regulations on data protection, as amended from time to time. Sign In Solutions and its Affiliates is registered as a data controller as defined in the UK GDPR with the data protection regulator in the UK, the Information Commissioner's Office.

There may be variations to our policy based on the product you are using, these are listed below:

Enterprise Ecosystem (SIE, SIC and SIW)

Standard Terms & Conditions: <https://signinenterprise.com/tos/>

Data Processing Agreement: <https://signinenterprise.com/tos/dpa/>

Sub-processors: <https://trust.signinenterprise.com>

Cookies: TBA

Sign In App and its Affiliated Companies (SIA, SICR, SISc)

Standard Terms & Conditions: <https://www.signincentralrecord.com/legal/terms>

Data Processing Agreement: <https://www.signincentralrecord.com/legal/data-processing>

Sub-processors: <https://www.signincentralrecord.com/legal/subprocessors>

Cookies: <https://www.signincentralrecord.com/legal/cookies>

Additional categories of data collected:

- Personal data entered by organisations in order to provide our service;
- Personal data inputted by Individual Users in order to use our services;
- Specific personal or personal-sensitive information, for example name, date of birth and gender;
- Personal contact information, for example address, telephone number and email address;
- and Information relating to the Individual User's use of our services such as booking and use of the Client's facilities, for example, membership or patient number.

Annex B - Regional and Industry Related Disclosures

There may be variations to our policy based on the country you are accessing our products from, these are listed below:

United Kingdom

Document Name: Privacy Notice
Document Number: SIS/IG/017
Version: 1
Date of Issue: 01/06/23

8. Where will your personal data be processed?

Where your personal data originates from the UK and is transferred outside the UK, it will only be transferred to countries that have been identified as providing adequate protection for EEA data, where approved transfer mechanisms are in place to protect your personal data or with an appropriate transfer mechanism in place such as 'Standard Contractual Clauses' or 'International Data Transfer Agreement', a contract and appropriate technical safeguards . If you wish for more information about this please contact privacy@signinapp.co.uk.

11. Data subject rights

If you're not happy with how we are processing your personal data, please let us know by sending an email to privacy@signinapp.com. We will review and investigate your complaint, and get back to you within a reasonable time frame.

You can also contact the Information Commissioner's Office on 0303 123 1113

or visit their website: <https://ico.org.uk/make-a-complaint/>.

EU & EEA

8. Where will your personal data be processed?

Where your personal data originates from the EEA and is transferred outside the EEA, it will only be transferred to countries that have been identified as providing adequate protection for EEA data, where approved transfer mechanisms are in place to protect your personal data or with an appropriate transfer mechanism in place such as 'Standard Contractual Clauses' or 'International Data Transfer Agreement', a contract and appropriate technical safeguards . If you wish for more information about this please contact privacy@signinapp.co.uk.

11. Data subject rights

If you're not happy with how we are processing your personal data, please let us know by sending an email to privacy@signinapp.com. We will review and investigate your complaint, and get back to you within a reasonable time frame.

You can also contact the European Data Protection Board

or visit their website: [European Data Protection Board](https://edpb.europa.eu/)

Document Name: Privacy Notice
Document Number: SIS/IG/017
Version: 1
Date of Issue: 01/06/23

Germany

We can provide you with a contract for order processing (Vertrag zur Auftragsverarbeitung (AVV)) please ask your sales representative.

US

8. Where will your personal data be processed?

Where your personal data originates from the US and is transferred outside the US, it will only be transferred to countries that have been identified as providing adequate protection for US data, where approved transfer mechanisms are in place to protect your personal data or with an appropriate transfer mechanism in place such as 'Standard Contractual Clauses' or 'International Data Transfer Agreement', a contract and appropriate technical safeguards . If you wish for more information about this please contact: privacy@signinsolutions.com.

HIPAA

Our products are HIPAA compliant and we can provide you with a Business Associate Agreement, please ask your sales representative for further details.

If you would like to do your own research on Global Privacy Law and Data Protection, the International Association of Privacy Professionals (IAPP) have a useful resource: <https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/>