



RETENTION POLICY

EFFECTIVE DATE: 10th February 2021

This policy sets out the various types of data we collect, process and store when providing our services, how long we hold that data for, and our reasons for doing so.

Our Retention Policy is just one of a range of policies we have that sets out how we at SoloProtect ensure your right to privacy is safeguarded. If you are looking for any of those other policies, you can find them here:

- [Privacy Statement](#)
- [Privacy Notice](#) (applicable to the use of the Website, www.soloprotect.com)
- [Privacy Policy](#) (applicable to the use of all SoloProtect services and SoloProtect Insights)
- [Cookie Policy](#) (applicable to the use of the Website, SoloProtect services and SoloProtect Insights)

SUMMARY

When we collect data through your use of our services, or information is shared with us by your Employer to provide those services, we hold onto different types of data for different periods of time.

Here, we have summarised the key things we think you should know about those periods (known as “retention periods”). For detailed information about our retention practices, our full Retention Policy follows this summary.

For any data directly relating to your use of our services, such as Key Personal Data, Location Data, and Incident Records, we retain this data for as long as you have a SoloProtect Device or SoloProtect Insights account with us. Once your account is deactivated or you are no longer using a SoloProtect Device, we delete your data after a fixed period following the end of your Employer’s contract with us; this is usually 2 years. We retain your data for this length because we are required to do so in accordance with the industry regulations and standards we must adhere to:

- BS 8591 (2014)
- BS 8484 (2016)

For Audio Communications Data, our retention periods are set by the type of the incident to which that data relates (i.e., “false” or “genuine”). Depending on the type of incident, our retention periods range from 3 to 12 months from collection.

Finally, for sensitive data such as your medical data, we only retain this information for as long as you have an activate SoloProtect Insights account and we delete this data immediately, but in any event no later than 90 days, from account deactivation.

At the end of the retention periods, we use secure processes to ensure your data is deleted.

SCOPE

This policy covers all personal data collected by us, shared with us by our customers (your Employer), or created using our services and covers the periods for which we store that data and our reasons for those retention periods.

This policy covers the retention practices of SoloProtect Limited and SoloProtect B.V as it applies to all personal data collected, process and stored by those companies relating to individuals who, through their Employer, interact with us or our services within the European Union.

GUIDING PRINCIPLES

At SoloProtect, protecting people is in everything we do and the trust your Employer places in us extends to our privacy practices. Those practices and our data retention practices are guided by the following overarching principles we at SoloProtect strive to adhere to:

- The data we collect, process, store and retain is required to provide our services effectively and legally, and we do not create or retain data for any other purpose outside the scope of those services.
- We comply with all legal and regulatory (both supranational and domestic) requirements to retain data.
- We comply with our data protection obligations, with the requirements to keep personal data for no longer than is necessary for the purposes for which it is processed.
- We handle, store, and dispose of data responsibly and securely and adhere to internationally recognised standards in doing so.
- We flow-down our data protection compliance measures to our partners and suppliers, as appropriate to the services they provide, and we regularly remind those partners and suppliers of their data retention responsibilities.
- All SoloProtect employees go through in-depth training on data protection compliance, and we regularly review and refresh that training.
- We regularly monitor and audit our compliance both against this policy and our entire suite of privacy policies and internal processes.

TYPES OF DATA WE RETAIN

Specifically, this policy applies to:

- **Account Representatives and Billing Contacts:** these are individuals responsible for the establishment of the contract with SoloProtect and its day-to-day operation, including ensuring that we meet our commitments, facilitating the purchase of SoloProtect Devices, resolving any issues should they arise or our principal contact for the purposes of receiving and paying our invoices.
- **Account Administrators and Escalation Contacts:** these individuals are responsible for the management of the services at the Employer as well as the key contacts we call should an incident occur with a Device User.

- **Device Users:** these are the individuals our services are designed to protect and include any individual the Employer (our customer) has issued a SoloProtect Device to.

| Data Type | Description | Applicable Individuals |
|--|---|---|
| Personal Master (or Key Personal Data) | Includes the information required to serve you with a SoloProtect Insights account including name, job title, company name, email address, contact telephone number, date of birth and gender. | Device Users Account Administrators Escalation Contacts (if provided with a SoloProtect Insights account) |
| Medical Data | Typically includes blood type, any known allergies, any known medical conditions, and any medication. | Device Users |
| Ethnicity | The ethnicity of the device user. | Device Users |
| Work Pattern Details | Includes work hours and place of work, as well as any other similar information. | Device Users |
| Vehicle Details | Includes vehicle type make, model, colour, and registration number. | Device Users |
| Other identity details | Includes other information used to identify an individual, such as height, weight, and physical description. | Device Users |
| Location Data | GPS coordinates of an individual's location. | Device Users |
| Audio Communications Data | Audio recordings of incidents captured over a SoloProtect Device. | Device Users |
| ARC or Incident Records | A written record made by our ARC Operators of incidents occurring over SoloProtect Devices. | Device Users Escalation Contacts |
| Key Contract Data | Information we collect from Account Representatives to allow us to manage the contractual relationship with our customer, including your name, job title, email address and contact telephone number. | Account Representative |
| Financial Data | Information we collect from Account Administrators and Billing Contacts to allow us to send invoices, receive payments and facilitate refunds and includes name, job title, email address and contact telephone number. | Account Representative Billing Contacts |
| Contact Data | Information we collect from Account Administrators and Escalation Contacts for us to provide our services, including name, job title, email address, contact telephone number. | Account Administrators Escalation Contacts |
| Contract Billing & Payments Data* | This information is predominantly corporate data (i.e., data about our customers, not about individuals), but it may still include personal information, such as your name, job title, place of work, contact details. | Account Representative Billing Contacts |

* We also collect and process corporate Cardholder Data, which may include personal information, however, we do not store/retain this information.

RETENTION PERIODS

The applicable data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed, and we have taken this principle and balanced it against our requirements, legal and/or regulatory obligations and legitimate interests when fixing our retention periods.

| Data Type | Retention Period | Reason |
|--|--|--|
| Personal Master (or Key Personal Data) | Contract + 2 years | Our industry regulations and standards require that we keep a full audit trail for at least 2 years from the end of the contract with your Employer. BS 8591 - 7.1 "Client Records should be kept for the duration of the contract plus two years" |
| Medical Data | Immediately, no later than 90 days from removal of your SoloProtect Insights account | We retain this information if you have an active SoloProtect Device and SoloProtect Insights account in order provide the services to you. |
| Ethnicity | Immediately, no later than 90 days from removal of your SoloProtect Insights account | We retain this information if you have an active SoloProtect Device and SoloProtect Insights account in order provide the services to you. |
| Work Pattern Details | Contract + 2 years | Our industry regulations and standards require that we keep a full audit trail for at least 2 years from the end of the contract with your Employer as this data provides circumstantial detail relevant to alarm handling. BS8484 – Data Retention 4.4.2 BS8591 - Client Records 7.1 a) "Details of... circumstances concerning the customer" |
| Vehicle Details | Contract + 2 years | Our industry regulations and standards require that we keep a full audit trail for at least 2 years from the end of the contract with your Employer as this data provides circumstantial detail relevant to alarm handling. BS8484 – Data Retention 4.4.2 BS8591 - Client Records 7.1 a) "Details of... circumstances concerning the customer" |
| Other identity details | Contract + 2 years | Our industry regulations and standards require that we keep a full audit trail for at least 2 years from the end of the contract with your Employer as this data provides circumstantial detail relevant to alarm handling. BS8484 – Data Retention 4.4.2 |

| | | |
|----------------------------------|---|---|
| | | BS8591 - Client Records 7.1 a) "Details of... circumstances concerning the customer" |
| Location Data | 2 years from collection | Our industry regulations and standards require that we keep all (data) communications to and from the ARC for at least 2 years. BS8591 7.5 "all [non-voice] data communications to and from the ARC... should be kept for at least two years" |
| Audio Communications Data | "Amber Alert/Check-In" - 3 months from creation False Alarm Audio - 3 months from creation Genuine Alarm Audio - (including associated telephone calls and "Amber Alerts"/"Check Ins") 12 months from creation. | - For false alarms: 90 days provides us with sufficient time to audit those alarms to ensure our reporting is accurate. - For genuine alarms: this is in line with our industry requirements. 'BS8484 - 7.1 "All verified alarm data and voice communications... should be retained for a minimum of 12 months." BS8591 - 7.4 "All voice communications to and from the ARC... should be kept for a minimum of three months" |
| ARC or Incident Records | 2 years from creation | Our industry regulations and standards require that we keep a full audit trail for at least 2 years from the end of the contract with your Employer. BS 8591 - 7.1 Client Records "records of all monitored events should be kept for not less than two years" |
| Key Contract Data | Contract + 2 years | We are required to retain this data as part of our regulatory, tax, insurance other applicable requirements in the various countries we operate in, such as for, such as fraud prevention. BS 8591 - 7.1 Client Records |
| Financial Data | 7 years from collection | We are required to retain this data as part of our regulatory, tax, insurance other applicable requirements in the various countries we operate in, such as for, such as fraud prevention. |
| Contact Data | Contract + 2 years | Our industry regulations and standards require that we keep a full audit trail for at least 2 years from the end of the contract with your Employer. BS 8591 - 7.1 Client Records |
| Contract Billing & Payments Data | 7 years from collection | We are required to retain this data as part of our regulatory, tax, insurance other applicable requirements in the various |

| | | |
|--|--|---|
| | | countries we operate in, such as for, such as fraud prevention. |
|--|--|---|

Please note that as it is our customer (your Employer) who acts as the Data Controller for most of this data, they may ask that we increase the above retention periods in certain finite circumstances. Where this is the case, we require them to inform you of this.

STORAGE, BACK-UP, AND DISPOSAL OF DATA

We store your in a safe and secure manner. We maintain a secondary data centre within our network, which we back-up your data to, to ensure we can get it back in the unlikely event it gets lost.

At the end of the defined retention periods, we use secure processes to ensure your data is deleted in line with the applicable EU standards for doing so (EN: 15713:2009)

For special circumstances, where we are obligated to retain data for longer than our stated retention periods (such as in the case of litigation, regulatory investigator, or audit) we ensure that your data is appropriately “put beyond use”. This means that we will not use that data in any way for our services, we will substantially restrict access to that data, and we will commit to permanently delete that data once we can do so.

YOUR DATA, YOUR RIGHTS

At any time you may request, through your Employer, the deletion of certain information we retain about you. On receiving such a request from your Employer, or, in the case of data where SoloProtect acts as the sole Data Controller, on receiving such a request from you, we will consider carefully that request and reply with an explanation as to why we are required to retain certain information either by law or for our own legitimate reasons. Where, after review, we identify any data we do not need to retain for these purposes, we will delete that data as per your request.

For any questions or comments about this policy or about SoloProtect’s data protection practices more generally, you can contact our Data Protection Officer as follows:

By email at: dpo@soloprotect.com

By post at: FAO DPO, SoloProtect Limited, Suzy Lamplugh House, 1 Vantage Drive, Sheffield, UK, S9 1RG.

We are regulated by the [Information Commissioner’s Office](#) under Z1252560 as our lead data protection authority and you can also contact them for advice and support.

UPDATES TO OUR POLICY

As we further enhance our product range and improve our services, we will be making changes to this policy and the other policies of our Privacy series. If we make any major changes, or any changes which directly affect our retention practices, we will notify of those changes. However, we encourage you to periodically review this policy for the most up to date version.