GROUP DATA PRIVACY POLICY

JULY 2022

Approved by the Group Management Team and Group Board

Executive Summary

This Policy sets the principles and rules to follow to protect *personal data* in our operations and continue earning the trust of our customers, colleagues and business partners.

Everyone at Verisure handles *personal data*. It is therefore critical that we all are aware of the principles and rules to follow for such data and comply with them in all we do.

Issuing Department: Group Legal Department

Owner: Chief Legal Officer

Version: 2.0

Introduction

Our continued success depends on our ability to maintain the trust of our customers, colleagues and business partners. These stakeholders trust us with their *personal data*. While our Code of Conduct sets general rules for the protection of customer and employee data, this Policy contains specific rules about how *personal data* is processed at Verisure. While it is the relevant Verisure Group entity that bears the legal responsibility for compliance with *data privacy laws,* it is crucial that we all ensure we comply with our internal policies and standards when processing *personal data* in our daily tasks.

Personal data is data relating to a directly or indirectly identified or identifiable person. Examples of *personal data* are name and surname, address, telephone number, ID number, email address, photos and video footage, date of birth, employment history, etc.

It is critical that we live up to the trust promise we make to the *individuals* whose *personal data* we *process.* Therefore, we will *process personal data* securely and in full compliance with this Policy and applicable *data privacy laws*. The new legal environment establishes clear responsibilities to us as a company processing *personal data*. In accordance with the accountability principle, we must also be able to demonstrate that we process *personal data* in full compliance with the applicable *data privacy laws* in the respective countries in which we operate.

This Policy provides the principles and rules that apply to all *personal data processed* by Verisure or its *processors* on Verisure's behalf.

All italicized words can be found in the definitions section of this document.

Other relevant documents

Throughout this policy, we have taken into account our :

- Group Code of Conduct
- Group Acceptable Use of IT Resources Policy
- Group Information Security Policy
- Group Information Security Incident Management Standard
- Group Classification and Handling Standard – User Guidance

Key Principles

***Processing personal data* lawfully, fairly and transparently**	We will process personal data lawfully. Examples of legal bases, which may be provided in applicable data privacy laws, are performance of a contract, compliance with a legal obligation, legitimate interest and consent.

	We will process personal data fairly which entails that we process personal data in a manner that individuals may reasonably expect their personal data to be processed, in particular in light of the information which we provide about our processing of personal data. We will process personal data transparently, always clearly informing individuals of how and for what purpose their personal data is processed.
***Processing personal data* for specified, explicit and legitimate purposes ("purpose limitation")**	We will only collect *personal data* for specified, explicit and legitimate purposes and we will not further *process* the *personal data* in a manner that is incompatible with those purposes. The purposes of *processing* should be determined before the *processing* of the *personal data* is initiated, i.e. *personal data* should not be collected "just in case we need it".
***Processing* adequate, relevant and necessary *personal data* ("data minimisation")**	We will only *process personal data* which is adequate, relevant and necessary for the purposes for which it was collected. This means that we should not *process* more *personal data* than necessary for a specified purpose.
***Processing* accurate *personal data* ("accuracy")**	We will keep *personal data* accurate, updating or deleting any inaccurate, outdated or incorrect information. We will have appropriate routines in place to ensure that the *personal data* we *process* is kept accurate.
***Processing personal data* only as long as necessary ("storage limitation")**	We will not store *personal data* for a longer period of time than what is necessary for the specified purposes for which the *personal data* is *processed.* We will identify relevant retention periods for *personal data* we *process* and will have relevant routines in place to implement such retention periods.
Ensuring appropriate security of personal data ("integrity and confidentiality")	We will keep *personal data* secure and protect it against unauthorized or unlawful *processing* and against accidental loss, destruction and damage, using appropriate technical and organizational measures. For example, we avoid unauthorized access to *personal data* by effective access control systems and, as relevant, access monitoring, encryption and other appropriate technical and organizational security measures.
Demonstration of compliance ("accountability")	We will be able to demonstrate our compliance with the *data privacy laws* by for example documenting our legal assessments relating to *processing* of *personal data* and relevant processes for *processing* of *personal data.*

Implementing privacy-by-design and privacy-by-default	All our products, services and processes are created and developed with privacy in mind. We will further reinforce this in the way we design, operate and manage our systems, products and services and by maintaining a "privacy first" culture.
Securing *personal data* transfers	We will only transfer *personal data* securely and with the required safeguards in place, in accordance with the applicable *data privacy laws* and after having consulted the Information Security team for guidance about tools and methodologies.

Who Must Follow this Policy?

We must all follow this Policy, as must our *processors that process personal data* on Verisure's behalf, even where local laws are more lenient. If local laws are stricter than this Policy, those laws take precedence over the Policy. In case of doubt, contact your *DPO, DPCC* or Legal function contact.

How Do I Comply?

Know how to identify *personal data*

Personal data is data relating to a directly or indirectly identified or identifiable person. Examples of *personal data* are name and surname, address, telephone number, ID number, email address, photos and video footage, date of birth or employment history, etc.

Personal data is a wide concept and any information having even indirect connection to identified or identifiable persons should be treated as *personal data* .

Please note that even pseudonymised data, i.e. *personal data* which has been de-identified by removing the direct identifiers such as name is still *personal data.* For example, a customer name could be replaced by a code in order to make it more difficult to connect certain information to a specific customer. While pseudonymisation is a useful security measure, the data must still be treated as *personal data.* Anonymised *personal data*, on the other hand, entails data that has been irrevocably anonymised by a destruction of the direct or indirect identifiers making re-identification of the data impossible. For example, statistics where any links with the original *personal data* is irrevocably removed may be considered anonymised data. Anonymised data is not *personal data.*

Processing* of *personal data

Controller determines the purposes and means of data *processing* and thus bears the responsibility for the data *processing*. The determination of who is the *controller* must be assessed separately for each data *processing* activity. In many cases the relevant Verisure Group entity is the *controller*. The Data Protection Officer or any other employee of Verisure is never the *controller*.

It is thus always the *controller* that is legally responsible for *processing* of *personal data* in accordance with the applicable *data privacy laws.* For individual employees, it is crucial that they comply with all relevant

internal Policies, Standards and Routines when they *process personal data* to ensure that we as a company comply with the *data privacy laws.*

Verisure has records of *processing* activities in place. The records of *processing* activities map all *processing* of *personal data* which is taking place at Verisure. Before initiating a new *processing* activity, the records of *processing* activities should be updated accordingly.

Important aspects of data *processing* are described below.

Legal basis

Whenever we *process personal data*, we must have a legal basis for doing so. A legal basis can be one of the following:

Consent	Consent can be a legal basis for *processing personal data*. Consent as a legal basis may be legally defined under applicable *data privacy laws* and each Verisure Group entity should be able to demonstrate that the use of consent as a legal basis fulfils the applicable regulatory requirements, including the right of the *individual* to revoke their consent. Consent should, unless other regulatory requirements apply for the relevant Verisure Group entity, be a freely given, specific, informed and unambiguous indication of the *individual's* wishes. This means that a consent should be requested separately and specific information about the consent should be provided in the context of such request. Generally, a consent remains valid for as long as there is no material change to the circumstances under which it was given. We will, however, provide *individuals* the possibility to withdraw their consent at any time. Consent will be used as a legal basis when no other legal basis can be used. This may be the case, for example, if Verisure wants to share successful customer cases as part of our marketing. In such case, a consent should be received from the concerned *individuals.*
Legitimate interests	Legitimate interest for *processing personal data* can be used as a legal basis when we assess that our or third party's interests in the *processing* override the interests or fundamental rights and freedoms of the *individual* which require protection of *personal data*. This assessment should be documented by concluding a so called Legitimate Interest Assessment (LIA). Legitimate interest is used as a legal basis for example when *processing* the *personal data* for the purposes of direct marketing or conducting employees' performance reviews. Please note that an *individual* may have an absolute right to opt out from direct marketing where the *processing* is based on the *controller's* legitimate interest under applicable *data privacy laws*.

Performance of a contract	Performance of a contract can be used as a legal basis when the *processing* of *personal data* is needed for the performance of a contract between Verisure and an *individual* (e.g., when selling to a customer, we can use his or her *personal data* to fulfil the terms and conditions and provide the services or when *processing* employees' *personal data* in order to pay salaries).
Compliance with a legal obligation	Compliance with a legal obligation can be used as a legal basis where the *controller* is subject to a legal obligation to *process personal data* for a certain purpose. An example of such legal obligation is relevant accounting legislation which obliges the *controller* to *process personal data*.
Processing of Sensitive Personal Data	In addition to a relevant legal basis, *processing* of *Sensitive Personal Data* requires additional protections, and we should know how to recognise and protect this data. *Sensitive personal data* should only be *processed* if such *processing* is allowed under applicable data privacy laws. Examples of *when* processing *of sensitive personal* data may be allowed are: - the *individual* has given his/her explicit consent to the *processing*; - it is necessary in the context of employment law or laws relating to social security and social protection (e.g., tax purposes); - it is necessary for establishing, exercising or defending legal claims (e.g., court orders); or - it is needed in order to comply with applicable laws.

Lifecycle of *personal data processing*

Once the grounds for *processing* of *personal data* are determined, we then take the following steps to protect it throughout its lifecycle in our company.

Privacy by design, privacy by default and review of new *personal data processing*

Privacy by design and privacy by default should start at the initial stages (i.e. Stage Gate 0 for product development) of any new business initiative. At this time, privacy should be taken into account (this is also known as privacy by design) and any default settings should put privacy first (this is also known as privacy by default)**.** For example, where possible, settings limiting the data collected to the minimum possible should be chosen. Privacy by design and by default incorporate adequate privacy protections to a new or modified business process, IT system, product, service or social media marketing platform. Security risk assessment are also required at this time to avoid security risk to *personal data*.

Privacy by design and privacy be default also apply to the way in which we work. We should ensure that processes within departments are checked to ensure compliance with privacy laws.

Risk assessments and *Data Protection Impact Assessment (DPIA)*

Before initiating new *personal data processing,* relevant risk assessments will be concluded. The purpose of such risk assessments is to evaluate whether the *personal data processing* is likely to entail high risk for the rights and freedoms of the *individuals*, more concretely whether the risks related to processing of *personal data* which may be detrimental to *individuals* are high. Based on the risk assessments, it will be assessed whether a full *DPIA* should be conducted before initiating *personal data processing.* At Verisure, these risk assessments may include one or more of the following depending on the *processing* at hand and any applicable local standards:

- Quick privacy assessment;
- Privacy assessment; and
- Data Protection Impact Assesssment.

A *DPIA* analyses and identifies ways to minimise the data protection risks. This should be done by the process owner in conjunction with the local *DPO* (and linking in with local Information Security team) using the DPIA assessment initiated by *DPO*).

If a *processing* activity cannot adequately protect the rights and freedoms of the *individual* after implementation, then seek guidance from your local legal and local *DPO*.

Privacy by purpose

We will only *process personal data* when specific and legitimate purposes have been identified in the records of processing activities and when those are clearly explained to the *individual*. For example, we *process personal data* for the following purposes (not exhaustive):

- Marketing and use of *online* presence;
- Bookings / installation & alarm services;
- Customer services / use of service;
- Administration of the customer contract;
- Refer a friend / member gets member;
- Third-party information sharing;
- Data transfer; and
- Ensure effective exercise of the rights of *the individuals*.

For a complete mapping of *processing* activities, please refer to the applicable records of *processing* activities.

Also, make sure that all the key principles are complied with when planning for a new *processing of personal data.*

Privacy by transparency

Verisure is required to be transparent and to inform *individuals* about what we do with their *personal data.* The guiding principle is that the *individual* should always be aware of our *processing* of their *personal data.* The main method of informing the *individuals* about how we *process* their *personal data* is through applicable *privacy notices,* which are addressed to different groups of *individuals* such as consumer

customers, business customers, website visitors, employees, etc.. Information about our use of cookies and similar technologies is provided in the applicable cookie notices.

Further, we will fufil the transparency requirement by providing additional information when appropriate in connection with a specific *processing* activity, for example by means of just-in-time notices. The transparency requirement should be considered before any new *processing* activity is initiated in the context of the privacy by design and privacy by default review.

Whether *personal data* is collected directly from the *individual* or through *third parties* is key for which information must be provided to the *individual* to help them understand how their *personal data* is being *processed*.

In the *controller's privacy notices*, we address all topics that follow from applicable *data privacy laws*, including the following:

- What *personal data* do we collect?
- How do we use *personal data*?
- What legal basis do we use to justify the *processing* of *personal data*?

Not only do we aim to use *personal data* in a legal and ethical manner, we always aim to be as clear as possible to the *individuals* on how we use their *personal data* in our company. Therefore, all of the *data processing* should be covered by the applicable *privacy notice.* If you have to *process personal data* for any purpose not stated in the applicable records of *processing* activities and in the applicable *privacy notice*, the records of *processing* activities and the *privacy notice* should be updated before initiating the new *data processing*. Further, the *individuals* should be informed about such update.

Privacy by security

We will take appropriate measures to ensure the integrity, availability and confidentiality of *personal data*. This includes protection against unauthorised or unlawful *processing,* accidental loss, destruction or damage.

Verisure has established security requirements in the relevant internal policies described in the section "Other relevant documents" to protect personal and confidential data. These must be applied by all parties, including business owners, and *application* and product developers.

Privacy by *processors*

When transferring or giving *processors* access to *personal data* controlled by Verisure, we will verify that *the processors* have adequate safeguards and procedures in place. For example, we should assess the safeguards and procedures that apply to the services they provide, such as Infosec policies, security measures including access and/or cryptography, system maintenance processes and incident management. We should only make data available if there is a data processing agreement in place with the *processor* in question, and this agreement should reflect the requirements of applicable *data privacy laws* and this Policy and we are comfortable that they have appropriate and effective controls in place for the type of data they are to *process*.

Privacy *online* and in *applications*

All *online activity and applications* from a Verisure Group entity will have transparent terms and conditions, and a specified *privacy notice*. This applies for example to sites such as the Verisure website, LinkedIn or Facebook profiles, as well as MyPages & MyMobile.

These documents should be based on Verisure Group templates, and then amended to take into account:

- The specific nature of the *online presence or application* in question;
- That *personal data* is *processed* in the context of that *online* presence or *application*;
- The requirements of applicable laws, including *data privacy laws*; and
- Any potential change in the purpose/scope previously communicated to *Users*;

Beyond the general principle of transparency, we will transparently inform the *users*:

- If we target an individual *user* with advertising (if we have received the ***user's*** consent for targeted advertising), about our marketing or promotional communication(s);
- About the use of "social plug-ins", "tracking pixels", or other cookie-type technology to provide personalized content or social experiences; and
- About the combination of *user personal data* with *personal data* collected through another *online presence, application,* or other source.

Cookies and similar technology usage

Users will be clearly informed of tracking technologies, like cookies or tracking pixels. Information about the use of cookies and similar technologies are provided in a cookie notice available *online*. For the use of non-essential cookies, we will receive the ***user's*** consent, which we request and document via a cookie banner.

The cookie notice provided to *users* should describe for example why their *personal data* will be *processed*, and how long it will be retained in compliance with regulatory requirements under the applicable *data privacy laws*. Above all, any tracking data placed on Verisure *User* devices should be encrypted.

Potential personal data breaches

Know what might constitute a potential *personal data* breach

Personal data breach means a breach of security where *personal data* is accidentally or unlawfully destructed, lost, altered, disclosed or accessed. Examples of *data breaches* include:

- Lost or stolen unencrypted devices (laptops, tablets, phones, storage devices), or paper records containing *personal data*;
- Databases containing *personal data* being hacked into, or illegally accessed by unauthorized *individuals*; colleagues, contracted staff or *processors* accessing or disclosing *personal data* outside the scope of their employment or engagement; and
- *Personal data* being accidentally provided to the wrong person, (e.g., by sending details to the wrong e-mail address, or sending out *personal data* that is not adequately protected).

Report any suspected *personal data* breaches

The most important first step in responding to a *personal data* breach is to immediately report any suspected breach to your local *DPO* or *DPCC* and to the local service desk (Eventum/Jira/Remedy). Under certain applicable *data privacy laws,* some of the data breaches must be reported to the competent Data Protection Authority within 72 hours, which means that it is important that any suspected breaches are reported to the *DPO* or *DPCC* and local service desk immediately. You should also let your manager know immediately in case there are commercial implications.

Refer to relevant internal policies described in the section “Other relevant documents” for more information.

Training

All Verisure Group entities will hold regular privacy-related training for all colleagues and contracted staff who *process personal data*. All colleagues should attend and take the opportunity to ensure they fully understand the contents of this Policy and the data privacy related internal rules applicable to their areas of responsibility.

Disclosing *personal data*

We will not disclose *personal data* to any *external party* unless we have a clear legal basis for doing so and the affected *individuals* are appropriately informed about such disclosure.

Third country* transfers of *personal data

We will take measures to ensure that any *personal data transferred* to a *third country* is adequately protected. The appropriate safeguards may be directed by applicable *data privacy laws*. These mechanisms should be in place before *transferring* to ensure that it is *processed* according to our policies.

Data retention and deletion

We should only keep *personal data* for as long as necessary for the purpose for which it was originally collected and in line with the *privacy notice* provided to, and, if applicable, the consent received from, the *the individual* in question.

Once *personal data* is no longer needed for any of these purposes, it must be anonymised, securely deleted, or destroyed.

Anonymisation* of *personal data

Personal data is anonymised when it is amended or aggregated so that it is impossible to identify a person. Once anonymised, it is no longer considered *personal data* and *data privacy laws* no longer apply. When making *personal data* anonymous, we have a responsibility that it is carried out correctly and is irreversible.

Rights of *individuals*

Individuals have a number of rights they may exercise as regards our *processing* of their *personal data*. Such rights are defined in applicable *data privacy laws* and include:

- Right of access;
- Right to rectification;

- Right to erasure (also known as the “right to be forgotten”);
- Right to restriction of *processing*;
- Right to notification regarding rectification or erasure of *personal data* or restriction of *processing*;
- Right to data portability;
- Right to object; and
- Right to not be subject to automated decision making and profiling using their *personal data*.

The rights apply to all *individuals* including our customers, prospective customers and employees. We should bear in mind these rights when we are *processing personal data* of *individuals* as, for example notes about them might have to be made available to the *individual* in question. We should also be aware that sometimes we cannot (legally) comply with an *individual*’s request. For example, if a previous customer asks us to erase all the details we have on them, we might still be required to hold details about their services contract for tax purposes. Therefore, it is important that any requests of *individuals* to exercise their rights are handled in accordance with applicable internal guidelines and routines.

Verisure is in some jurisdictions legally obligated to facilitate the rights of their *individuals* in a timely way, as a rule within one month from receipt of the request. Therefore, appropriate mechanisms should be in place to identify and respond to *individual*’s requests. We can respond to *individuals* requesting to exercise these rights only once the *individual* in question has been appropriately identified. We should then ensure that our responses are secure and appropriate for the situation and in compliance with the legal requirements. Communication to *individuals* should be directed through the usual channels. This means that employees should be responded to via HR and that customers are contacted through the usual customer servicing channels.

Who does what?

Function	Responsibilities
Group Management Team	Group Management Team bears the overarching responsibility for Group level compliance with *data privacy laws.* Group Management Team ensures that Group data privacy risks are identified, understood and managed. They also create risk-based approaches for the Country Management Teams to work within and oversee the creation of a risk management culture across the Group.
Country Management Teams	Country Management Teams bear the overarching responsibility for the country level compliance with *data privacy laws.* Risk management is an operational responsibility. Each country management team is responsible for identifying, mitigating and managing the data privacy risks that apply to their business. This includes appointing a *DPO* or *DPCC* as appropriate in their countries. The Country Management Teams are also responsible for ensuring sufficient data privacy governance, for example that the Group Policies and Standards are appropriately implemented and that local steering documents are adopted where necessary.

Group Data Privacy Team and Group Compliance Team (Group Legal)	Group Data Privacy Team belong to the Group Legal and is responsible for the design, management and implementation of Verisure's privacy program. The Data Privacy Team is also responsible for designing the framework, organisation, policies, standards and guidance for compliance with this Policy and, as part of complying with this Policy, with *data privacy laws.* Finally, the Data Privacy Team provides support to the country organisations and the functions of the Company in all data privacy related questions. Group Compliance Team also belongs to Group Legal and is responsible for data privacy compliance measures such as incorporating data privacy risks as part of enterprise risk management assessments, facilitating training and policy roll outs, etc.
Country Data Protection Officer (DPO) and Country Coordinators (DPCC)	Each Country has an appointed *DPO*. The *DPO*'s tasks include: - Providing information and advice for the *controller* and the employees *processing personal data,* - Monitoring the compliance with the *data privacy laws* and the relevant internal steering documents, - Providing advice where requested as regards the *DPIAs* and monitoring its performance, - Providing data protection related training within the organisation, - Participating in the management of potential data breach situations, - Cooperate with the *Supervisory Authority* and act as a contact point for the *Supervisory Authority* and, - Handling any privacy related questions, requests or complaints from *individuals*. The *DPO* shall be registered with the local *Supervisory Authority* and reports on privacy issues to the local management team. The *DPO* is responsible for understanding the main data flows within a Verisure Group entity or country. If a *DPO* is not appointed in the relevant Verisure Group entity, which may be the case in countries outside of the EU/EEA, a *DPCC* shall be appointed instead. *DPCC* will have similar tasks as a *DPO.* The *DPO* or the *DPCC* have an advisory role and they are active in contributing to Verisure's compliance with the *data privacy laws.* Any decisions will be, however, made in accordance with the applicable decision-making mandates in the operative part of the organisation.
Managers	Are responsible for ensuring their line reports understand and comply with privacy related policies and for liaising with the local *DPO* to inform them of changes to data *processing* within the organisation.

Colleagues	The behaviour of Verisure employees, contractors and other staff are vital to implementing our policies and complying with d*ata privacy laws*. This includes identifying and telling the right people about any material data privacy risk or an actual or suspected data breach. Breaches are to be recorded with the local service desk, in addition to telling your local *DPO*.

It is vital that we are guided by the culture and risk behaviours mentioned in this document. In doing so we develop greater awareness and trust amongst ourselves, and with our customers.

Questions and Support

At Verisure everyone handles personal data one way or another. It is critical that we all live up to the trust promise that we make to our customers, colleagues and others whose personal data we process. If there are any questions or a need for support, do not hesitate to consult with any of the following resources:

- The Intranet or the Local Service Desk – for example by accessing the Verisure privacy knowledge base via the Intranet or creating a privacy ticket in the region's Service Desk Ticketing System (e.g., Jira);
- The *DPO* or *DPCC* in your country;
- The local legal function; or
- The Group Data Privacy Team at dpo@verisure.com.

Definitions

Anonymisation	The process of irreversibly removing personal identifiers, both direct and indirect, rendering the Personal data anonymous in such a manner that the individual is not or is no longer identifiable.
Controller	The person/company that decides the purposes and means, or in other words how and why *personal data* is *processed*. Usually the *controller* is a Verisure Group entity collecting and using the *Personal data* .
Data privacy impact assessment (DPIA)	An assessment of a *processing* activities' impact on the protection of *personal data.* This is done when the conclusion of a risk assessment, which is to be done before any *processing* is initiated, where the *processing* is likely to create a high risk to the *individuals'* rights and freedoms.
Data privacy laws	The applicable privacy and data protection legislation that applies in the respective jurisdiction where a Verisure Group entity operates. For example, in EU countries, the General Data Protection Regulation (EU)

	2016/679 (“GDPR”) and any complementary data protection related legislation are the basis for Verisure’s compliance with applicable *data privacy laws*.
Data Protection Officer (DPO) and Data Protection Country Coordinator (DPCC)	*DPO* is the person appointed under the GDPR to independently carry our privacy related tasks as specified by the *data privacy laws.* The *DPCC* has a similar role in those jurisdictions where the GDPR is not applicable.
Individual	The specific person to whom the *personal data* relates (also known as “data subject” in some laws, such as the GDPR).
Online and Applications	A resource used by, or on behalf of, any Verisure Group entity that creates engagement with *users* (e.g., Verisure websites, mobile phone *applications*, Facebook pages and Twitter accounts).
Personal data	Information concerning an *individual* (e.g., name, address, telephone number, government identity number, e-mail address, date of birth, IP address, personal account number, company user ID etc.).
Privacy notice	The information given to *individuals* about the *processing* of their *personal data* as required under GDPR. It informs them of the types of *personal data* collected by the *controller*, how the *controller processes* the *personal data*, the purpose of *processing* their *personal data*, etc. Some countries refer to it as a ‘legal notice’.
Process, Processing or Processed	All activities, involving the handling of *personal data*. The activities can be large or small, direct or indirect. This includes the access, collection, storage, transfer, use, disclosure, retention, amendment, erasure, deletion, reviewing, passive storage and any other operation involving *personal data.*
Processor	A person or company that *processes personal data* on behalf of, and in accordance with, the *controller*’s instructions (i.e., an external entity, such as another Verisure Group entity)
Profiling	Automated *processing* that uses *personal data* targeted to evaluate someone’s performance, capability, preference, economic situation, health interest, reliability, behaviours, location and/or movement.
Recipient	Anybody who receives data, or to whom *personal data* is disclosed. This does not apply to the *controller*.

Supervisory Authority	Regulatory body or authority with jurisdiction to regulate and oversee data privacy compliance.
Sensitive personal data	*Personal data* involving the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, physical or mental health, sex life, sexual orientation, the act or alleged act of any offence and its related proceedings and outcome.
Third country	Any country outside of the European Economic Area.
Third party	Any entity, other than the data subject (in this Policy called *individual)*, *controller*, *processor* or persons who, under the direct authority of the *controller* or *processor,* are authorised to *process personal data* .
User	Someone engaging with Verisure *online* and/or in an *application* where *personal data* is provided.

Version Control

Version History

Version	Effective Date	Description of Change	Status	Author
1.0	May 2019	Original document	Replaced	Group Legal
2.0	July 2022	Key revisions include the following: - Clarifications relating to the anonymization of personal data, legal basis for processing personal data and responsibilities of certain key internal functions; - Additional information on risk assessments and transparency requirements; and - Strengthened language on the importance of privacy and personal integrity within the Company.	Approved	Group Legal

Approval Trail

Version	Policy Owner		Formal approver	
	Date	*Name*	*Date*	*Name*
1.0	May 2019	Group CLO	May 2019	Group Management Team
2.0	July 2022	Group CLO	July 2022 September 2022	Group Management Team Group Board