

PRIVACY STATEMENT ENC SECURITY

WHAT IS THE GDPR

On May 25, 2018, the **General Data Protection Regulation (GDPR)** took effect in the European Union. The GDPR governs how both “Data Controllers” and “Data Processors” collect and process “Personal Data” of EU citizens (“data subject”). Based on well recognized privacy principles of accountability, fairness and transparency, GDPR brings long awaited consistency to data protection in the EU by harmonizing the existing patchwork of national data protection legislation across all EU member countries.

ENC SECURITY B.V. AND ENC SECURITY SYSTEMS LLC

This privacy statement is applicable on both ENC Security B.V., a Dutch company, as ENC Security Systems LLC, the US subsidiary of ENC Security B.V. Both are referred to as “ENC”.

ENC controls and processes personal data of clients (including their clients) and staff. ENC wants to ensure a secure and safe controlling and processing of private personal data and safeguards, protects and guarantees privacy. The purpose of this statement is to clarify what the laws and regulations concerning private data imply for ENC, for its the customers, partners and staff.

Our customers and staff should rely that ENC handles their data carefully, fair and transparent. ENC is dedicated to helping our customers, partners and staff navigate GDPR by protecting and respecting personal data, no matter where it is collected or processed, and is committed to compliance with applicable regulatory frameworks wherever, including GDPR and local laws.

This privacy statement can be adjusted from time to time if reviews necessitate this.

PURPOSE AND LEGAL BASIS OF USING PERSONAL DATA

Under GDPR, there are six different legal bases under which personal data can be processed. It is ENC policy to identify the appropriate legal basis for data processing and document it. These are briefly described below:

1. Consent

ENC will collect and process the personal data with consent by data subjects. This consent must be revocable at any time.

2. Performance of a Contract

Where personal data is collected and processed required to fulfil a legal contract with the data subject or to take necessary steps at the request of those concerned prior to entering into a contract, then explicit consent is not required. This also applies where ENC has signed a legal contract with a client for the provision of our Software and Consultancy services and solutions and the data subjects’ personal data is necessary for completion of the contract. Note that where the client is not an individual, or where the client is not the same person as the data subject, the client will be required to confirm that it has a legal basis for providing the information on the data subject to ENC.

3. Legal Obligations

Where ENC is acting as a Data Controller it is required to collect and process a data subject's personal data in order to comply with a legal obligation such as an EU member state's employment or taxation legislation, then explicit consent is not required from the data subjects to process the data required.

4. Vital Interests of a Data Subject

Where personal data is required to be processed in order to protect the vital interests of the data subject or of another natural person, then such processing is regarded as lawful under the GDPR. ENC will retain reasonable documented evidence to cover this case whenever this reason is used as the lawful basis for this type of processing of personal data.

5. Public Interest Tasks

Where ENC is required to perform a task that we believe is in the public interest as laid down by law or as part of an official duty, then explicit consent is not required from the data subjects. The assessment of the public interest task or official duty will be documented by ENC.

6. Legitimate Interests

If the processing of specific personal data is in the legitimate interests of ENC and a proportionality assessment is carried out that determines that ENC legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject, then this may be defined as the lawful basis for processing. This will be documented by ENC.

PERSONAL DATA PROCESSED BY ENC

Whenever an individual engages with ENC, personal data can or will be processed by ENC. Different situations are applicable for ENC:

1. Visiting our website – this involves processing user behavior, IP and possibly cookies
2. Buying our products – this involves processing name, email address, payment details, IP address
3. Using our contact form – this involves processing name, phone number, email address and the contents of the message
4. Signing up for our newsletter – this involves processing email address

We are processing this data to enable you to use our website, perform a contract or based on a legitimate interest of ENC. We will not store your data longer than necessary for the goal and reason we've collected and processed your data.

RIGHTS OF THOSE CONCERNED

Each data subject can request to exercise the following rights under the GDPR with respect to the controlling and processing of their personal data:

1. The right to be informed.
2. The right to access the personal data processed.
3. The right to rectification of inaccurate personal data concerning him or her.

4. The right to erasure of the personal data where there are legitimate grounds for retaining it.
5. The right to restrict processing.
6. The right to receive the personal data provided to a controller concerning him or her (data portability).
7. The right to object processing of personal data concerning him or her.
8. The right not to be subject to automated decision making and profiling rights.

Requests to exercise these rights should be generally handled in one month and sent to privacy@encsecurity.com.

DATA TRANSFERS

ENC operates in various countries and where legally permissible, ENC may store, use, transfer, and otherwise process personal data of staff, customers in countries outside of the country of their residence, which may have different data protection rules.

ENC may transfer and/or disclose personal data of its staff and customers to any company within ENC and to specific third parties acting on ENC's behalf. Such intra-group international data transfers will be subject to legally binding agreements, which provide enforceable rights for data subjects.

This also includes processing data outside the European Economic Area. ENC may transfer personal data outside the EEA to a third country or international organization that does not provide an adequate level of data protection, only with explicit consent.

ENC will ensure that all (processing and (sub)processing) agreements it enters into with our clients, service providers or others, that involve the processing of personal data, are subject to a documented legal contract that includes specific provisions and terms as required by the GDPR.

BREACH NOTIFICATION

GDPR requires ENC to notify relevant Data Protection Authorities (DPAs) within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of impacted data subjects. ENC must also notify impacted data subjects without undue delay when a high risk to rights and freedoms is likely. ENC as a processor must notify their clients (Data Controller) of a data breach without undue delay. As ENC Security B.V. is established in Amsterdam, the Dutch DPA is ENC's lead authority.

CONTACT

Questions, remarks or other requests about our data collection, privacy statement or the way we handle personal data, can be send to privacy@encsecurity.com.