

Future Security Systems Ltd

GDPR General Data Protection Regulations

Privacy Policy – Amended 25th May 2018

We are Installers of Security Systems and registered with the SSAIB.

We are committed to safeguarding your privacy. This policy set out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

Definitions:

Future Security Systems Ltd (“we”, “us”, “our” or Future), registered office Berkeley Hall Ltd, D2 Southgate, Commerce Park, Frome, BA11 2RY. “User” “or” “you” or “your” “customer” refers to you, as a user of Future Security Systems Ltd.

Data Controller:

Future Security Systems is a “Data Controller”, which means that we are responsible for deciding how we hold and use personal information about you. We are required - under data protection legislation – to notify you of the information contained in this privacy notice.

It is important that you read this notice so that you are aware of how and why we are using such information.

Personal Data we collect:

“Personal data” is information that can be used to uniquely identify or contact an individual and includes a variety of information such as your name, postal address, phone number, e-mail address and contact preferences.

When using our website, we may also use certain performance tracking tools, such as Google Analytics. Through the use of Google Analytics we gather information regarding your behavior and preferences when using our online platform.

Why do we need this information?

We collect your personal data for various legitimate business purposes only. We only collect the information we need to fulfill the business purpose.

Notice and Choice:

We will notify you about the types of personal data we collect, the purposes for which we collect such information and the types of third parties to which we disclose such data.

We may use your personal data to:-

- List details on our database - for the purposes of awarding and maintaining certification.
- Contact you for scheduling appointments
- Sending quotations, certification and project related materials
- Sending invoices
- Sending you contract information
- Reissue correspondence.
- Comply with our statutory and regulatory obligations.
- Where we need to perform the contract, we are about to enter into or have entered into with you.
- If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

We will only use your personal data when the law allows us to.

What do we do with this information?

Your information is stored securely, both electronically and through paper filing systems.

Others:

Future Security Systems may disclose personal data if necessary by law such as litigation, or request or subpoena from public and governmental authorities within or outside your country of residence.

We may also disclose information about you if we determine that for purposes of national security, law enforcement, legal compliance, or other issues of public importance, disclosure is necessary or appropriate.

Future Security Systems may disclose information about you if we determine that disclosure is reasonably necessary to enforce our terms and conditions, or other contractual or legal rights, or to protect our operations or employees. Additionally, we may disclose your personal data to a third party if we file bankruptcy, or there is a transfer of assets or ownership in connection with proposed or consummated corporate reorganizations, such as merger, acquisition, sale or other disposition of business units.

How Secure is my Data?

There are always risks with providing personal data, whether in person, by phone, via the Internet or otherwise, and no technology is completely safe or "hacker" proof. Future Security Systems takes appropriate technical, administrative and organizational informational security measures to prevent and minimize such risks.

Such measures include, where appropriate, the use of firewalls, secure server facilities, encryption, implementing proper access rights management systems and processes, careful selection of processors and other technically reasonable measures to provide appropriate protection for your personal data against unauthorized access or disclosure. Where appropriate, we may also take backup copies and use other such measures to prevent accidental damage or destruction to your personal data.

Your rights**Integrity and Retention of Personal Data:**

Future Security Systems will retain your personal data for the period necessary to fulfill the purposes described in this Privacy Statement unless a longer retention period is permitted by law.

For other personal data we make good faith efforts to provide you with access so you can request that we correct the data if it is inaccurate or delete the data if Future Security System is not required to retain it by law or for legitimate business purposes.

We may decline to process requests that are unreasonably repetitive, require disproportionate technical effort, violate the privacy of others, or for which access is not otherwise required by local law.

If you wish to make requests to access, correct, or delete personal data please contact email info@futuresecuritysystems.com

Under certain circumstances, by law you have the right to:-

- Request access to your personal information. This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing hold this.

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

Your right to Complain

If you have any problems with the way that we are handling your personal data, you should contact the Information Commissioner's Officer (ICO).

The ICO can be contacted by telephone on 0303 123 113 Monday – Friday, between 9am and 5pm – or by email at casework@ico.org.uk You can also visit the ICO's website by following this link <https://ico.org.uk/>.