

Introduction

Definitive Security Solutions is a private security company that supports many UK companies and is authorised by its customers to perform installations, service, consultancy, and loss prevention duties across their estates.

Definitive Security Solutions gathers information from its customers, its employees and partners and stores it in a few software platforms including its own software, when necessary, and to prevent crime, shares its intelligence with customers, its employees and the police. Definitive Security Solutions collects information from its customers, employees, and partners about individuals who:

Have committed criminal offences or attempted to commit offences against its customers or their employees including violence and/or

Have exhibited anti-social behaviour, within or around a customer's premises or property.

The information collected contains Personal Data which may include data relating to suspected offences.

Once received from a customer, an employee, a partner, or the police, Definitive Security Solutions stores the information in its secure software, and shares certain elements of it with other employees, customers, and the police when this is justified, proportionate, necessary and fair and lawful to do so.

Definitions

Controller – Definitive Security Solutions Limited is the organisation which determines the purposes and means of the processing of personal data.

Processor – A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Recipient – A natural or legal person, public authority, agency, or other body, to which the personal data is disclosed, whether a third party or not.

Third Party – A natural or legal person, public authority, agency, or other body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Personal Data – Any information relating to an identified or identifiable natural person ("Data Subject") An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category Personal Data – Any information relating to an identified or identifiable natural person ("data Subject") which falls into one of the following categories. Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life, data concerning a person's sexual orientation.

Data Subject – Any identifiable natural person, who's personal data is processed by the controller responsible for the processing.

Definitive Security Solutions – Company

Customer – Definitive Security Solutions Client

Partners – Organisations with which we may share your data.

SOI – Subjects of Interest are individuals who are suspected of, or have committed crime against our customer or employees.

How to contact us

If you wish to contact us in relation to this privacy notice or if you wish to exercise any of your rights (described below) then please address your correspondence to.

Definitive Security Solutions: Unit 11 Park Road Industrial Estate, Park Road, Swanley, Kent BR8 8AH

Alternatively, you can email us at dpo@Definitivesecuritysolutions.co.uk

We have also appointed a Data Protection Officer (DPO), if you do send correspondence by post please mark the envelope to the 'Data Protection Officer'.

Our Data Protection Officer

The Data protection officer can be contacted by emailing dpo@Definitivesecuritysolutions.co.uk.

Reason for processing your data

Definitive Security Solutions is contracted by its customers to protect life, protect property and premises, prevent crime including violence and threats of violence and prevent loss and waste.

We do this by detecting crime or suspicious behaviour, preventing crime and apprehending individuals who commit crime against our customers or employees.

Some examples of how Definitive Security Solutions can achieve this are set out below:

Definitive Security Solutions can collate, and link offence data provided by individual Definitive Security Solutions customers and our employees. This means offence data can be collated and provided to the police or our partner organisations such as the National Business Crime Centre (NBCC) as series linked investigations, making it more likely that an offender will be apprehended through police action. Such reporting makes eventual apprehension much more likely than individual reporting of crimes to the police by Definitive Security Solutions customers.

Definitive Security Solutions customers, and employees are more likely to report known or suspected offenders to Definitive Security Solutions than to the police. Definitive Security Solutions is able use such offence data provided by its customers to identify and analyse trends and generate reports and analysis. This in turn helps Definitive Security Solutions, the police and the customer develop better strategies for dealing with crime.

Definitive Security Solutions can identify prolific and persistent offenders targeting multiple businesses and can assist its e and customers in serving exclusion notices against these individuals removing their implied right to enter those businesses or private property such as in customer stores or on retail parks.

This in turn reduces the likelihood that those individuals will re-enter those business premises and property and commit further crimes. Additionally, should that individual breach the exclusion notices then the Definitive Security Solutions can support that customer, or a group of customers in applying for a civil court injunction or support the Police in obtaining Criminal Behaviour Orders or pass the data to a trusted partner link Retail Loss Prevention. This action further prevents the individual from entering the customer premises and if breached can constitute contempt of court.

By sharing proportionate actionable intelligence with its employees and customers, Definitive Security Solutions can support customers, thereby reducing crime and the risk of crime and anti-social behaviour within their stores, premises, or property.

By conducting their work, Definitive Security Solutions wish to achieve a reduction in criminal activity within the retail, commercial and distribution sector and create a safer experience for both their employee's and consumers. Definitive Security Solutions is already demonstrating achievements as highlighted above, and, therefore, with the support of all interested parties including the police needs to continue with this work.

What Data do we collect and process

To achieve our purpose, we may collect the following data:

- Name and address details
- Images taken from CCTV
- Video taken from CCTV
- Images taken from Body Worn Video
- Images taken from CCTV for the purpose of live facial recognition supporting identification of offenders or suspected offenders
- Images taken from Body Worn Video (BWV) for the purpose of live facial recognition supporting identification of offenders or suspected offenders
- Date of birth, age and descriptive details such as tattoos, facial hair, eye colour, hair colour, height, build clothing , piercings, glasses and other identifiable features.
- Gender
- Email address
- Phone number
- Details of associates
- Vehicle Registration Details for the purpose of automatic number plate recognition
- Any records of correspondence

We may also process special category data, which is data of a more sensitive nature, the following data types may apply:

- Race and or ethnic origin

- Details of suspected criminal offences
- Details of civil action taken against individuals

Definitive Security Solutions facial recognition system uses facial recognition technology to identify subjects of interest who we have good reason to believe have committed an offence against one of our customers or employees.

Images are collected by our employees during their normal course of duty of individuals who have or are highly likely to have committed an offence against our customer or our employees. Following a match our software will alert our employee(s) that there is a high likelihood that the image matches a subject of interest.

Before any action is taken against the subject of interest the employee must confirm the image identified matches the subject, there is therefore human intervention at every stage of this process and no decisions which may impact the data subject are made on an automated basis.

Definitive Security Solutions has robust processes and training in place to ensure this process is followed each time a potential match is identified.

In order for facial recognition to be successful we must process data on subjects of interest, and members of the public. When you interact with our employees your image will be taken by the software and compared to the Definitive Security Solutions watch list, if there is no match against the database then your image is immediately and irrecoverably deleted, this happens in an instant meaning there is no risk to data subjects who are not subjects of interest.

We consider this process to be less intrusive than store CCTV, store CCTV captures your data and stores it for 31 days, often on internal store hard disks.

Rights of the data subject

UK GDPR affords you with a number of rights, your rights are summarised below. Definitive Security Solutions are committed to supporting you with these rights where required and so you may contact our designated Data Protection Officer dpo@Definitivesecuritysolutions.co.uk or any employee at any time to exercise these rights.

The right to request access – you have the right to obtain from Definitive Security Solutions free information about your personal data and a copy of the personal data we store (commonly known as a “Subject Access Request”), furthermore you have the right to obtain information as to whether your personal data is transferred to any third countries or international organisations. Where this is the case, you have the right to be informed about any safeguards relating to this transfer.

Right to rectification – You have the right to obtain from Definitive Security Solutions without undue delay the rectification of inaccurate personal data concerning you. Basically, if we hold incorrect data about you, you have the right to have that data corrected.

Right to erasure (right to be forgotten) – UK GDPR grants you the right to have your data deleted when there is no good reason for us to continue to process it. Definitive Security Solutions have an obligation to erase your data without undue delay where one of the statutory grounds applies, as long as the processing is not necessary. Definitive Security Solutions relies on

Legitimate Interests as its lawful basis and therefore the processing of your data is necessary to achieve our purpose. For this reason, the right to erasure does not apply in every instance.

Right of Restriction of Processing

You have the right to obtain from Definitive Security Solutions a restriction of processing where a statutory reason applies. This enables you to ask us to suspend processing your data, for example if you want us to establish its accuracy or the reason for processing it.

Right to data portability

You have the right to receive personal data we process concerning you in a structured, commonly used, and machine-readable format. You have the right to request the transfer of your data to another party.

Right to Object

You have the right to object to us processing your personal data, on grounds relating to your situation at any time. This does not mean that we will stop processing your data, but we will review your objection in each case.

Automated individual decision-making, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling.

Right to withdraw consent

Definitive Security Solutions does not use consent as the legal basis for processing, we use legitimate interests for this purpose, therefore you do not have the right to withdraw consent.

Right to complain to the supervisory authority

The contact details for the ICO are contained in this privacy notice.

How to exercise your rights

You will not usually pay a fee to access your personal data or to exercise any of your other rights. We may charge a reasonable fee if your request for access is unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances. If you wish to exercise your rights, then please contact us at dpo@Definitivesecuritysolutions.co.uk.

What is our legal basis?

Definitive Security Solutions uses the lawful basis “legitimate interests” for processing your data as the processing is necessary to protect the business interests of our customers and there is no less intrusive method to achieve those business interests. Our legitimate Interest is not outweighed by the rights and freedoms of the affected data subjects as our processing is for the substantial public interest, the benefit of Definitive Security Solutions, its customers and consumers.

Where we process Special Category Data, such as biometric data for the purpose of live facial recognition, we do so on the basis that it is necessary for the substantial public interest, in

accordance with Article 9 (2) (g) of the UK GDPR. We have assessed this interest against the appropriate provisions within the Data Protection Act 2018 (DPA 2018) and considered that our processing is necessary for the provision of detecting an unlawful act, in accordance with paragraph 10, schedule 1 of Part 2 of the DPA 20218.

Personal data and retention periods

Most of your personal data will be held for 24 months before it is permanently and securely disposed of. The secure disposal of your data is an automatic process removing the risk of human error. All personal data is held in UK based secure servers.

Your biometric data used for live facial recognition will be disposed of after 12 months.

Your vehicle registration mark data will be disposed of after 3 months.

Your images held on body worn video for the protection of our Employees will be disposed of after 31 days.

Security of processing

As the Data Controller Definitive Security Solutions have implemented appropriate technical and organisational measures to ensure your Personal Data always remains secure.

How to contact the ICO

You have the right to lodge a complaint with the supervisory authority if you believe we are infringing UK data protection laws or you are concerned about the way in which we are handling your personal data, in the case of the UK this is the ICO.

You can contact the ICO by following this link <https://ico.org.uk/global/contact-us/> or by telephone on 03031231113.

Changes to this notice

This notice was last updated on 02/01/2024. We may change this notice by updating this page to reflect changes in the law or our privacy practices at any time.