

Privacy Notice for Offenders

Introduction

GO! Southampton (referred to as "GO! Southampton" "We, "Our" or "Us") are committed to protecting the privacy and security of your Personal Data.

We have developed this Privacy Notice to inform you of the data we collect when an offender has their personal data processed by us. It is important that you read this notice, along with our other privacy notices as applicable, so that you are aware of how and why we are using such information.

Definitions

For the purposes of this notice:

Company (referred to as "GO! Southampton", "the Company", "We", "Us" or "Our" in this Agreement) refers to GO! Southampton Network Eagle Lab, Portland Terrace, Southampton, SO14 7SJ registered with the ICO under ZA363052.

Data Controller for the purposes of both UK and EU GDPR, refers to the Company as the legal person which alone or jointly with others determines the purposes and means of the processing of Personal Data. For both UK and EU GDPR, the Company is the Data Controller.

Data Processor for the purposes of both UK and EU GDPR, refers to the Company's Service Providers.

Data Protection Legislation refers to the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018.

Member means any business who are a member of the Southampton Business Crime Partnership.

Offender means individuals aged 14 years and over who have been reported to have been actively involved in incidents which have presented a threat or damage to the property or safety of Members or Members' staff or customers.

Personal Data is any information that relates to an identified or identifiable individual. For the purposes of both UK and EU GDPR, Personal Data means any information relating to you such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity.

Data Protection Legislation

Throughout this document we refer to Data Protection Legislation.

Where data is processed by a controller or processor established in the European Union (EU) or comprises the data of people in the European Union, it is subject to the General Data Protection Regulation (Regulation (EU) 2016/679) ('EU GDPR') as well as any local data protection implementation laws. This includes any replacement legislation coming into effect from time to time.

In the United Kingdom (UK), Data Protection Legislation means the Data Protection Act 2018 ('DPA 2018'), United Kingdom General Data Protection Regulation ('UK GDPR'), the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') and any legislation implemented in connection with the aforementioned legislation.

GO! Southampton SBCP is the Data Controller ('controller') for the Personal Data we process, unless otherwise stated.

You can contact us either by phone, email, or post.

Our main trading/postal address:

GO! Southampton

Southampton Business Improvement District Ltd
Network Eagle Lab
Portland Terrace
Southampton
SO14 7SJ

Phone: 02380 003637

Email info@gosouthampton.co.uk

Our Data Protection Officer: Stephen Manion and can be contacted by email at stephen.manion@gosouthampton.co.uk

Do we process your personal data?

This privacy notice is intended for only those persons reported to have been actively involved in incidents which have presented a threat or damage to the property or safety of Members or Members' staff or customers.

The information we collect

The personal data that we may collect about you is as follows:

- Name
- Still images
- Moving images – video recording footage
- Date of birth
- Descriptive details
- Email address
- Phone number
- Vehicle registration details
- Information and evidence about incidents in which an offender has been involved.

We may also process other sensitive personal data relating to racial or ethnic origin, religious or philosophical beliefs, health, sexual orientation, and criminal offences or allegations to the extent that this data is visible in the images or audio recorded by our cameras or on the exclusion list details.

We may collect this data from you directly or we may receive it from UK law enforcement bodies, our business members, open-source material via social media and any other relevant bodies or businesses linked to ongoing criminal investigations.

Where data is collected directly from the offender:

- The offender will be served a warning letter which will give information on how to obtain a copy of this privacy notice (offender) at the time and place of data collection if practicable. If

this is not practicable the offender will be directed on how they can access this information from <https://www.discnet.org/gosouthampton> and <https://www.gosouthampton.co.uk/>

How we use your information

We will only process your Personal Data when the law allows us to do so. The Personal Data will be used to:

- detect, deter, and mitigate the potential of crime or criminal offences (including assault and threats of assault as well as verbal abuse and criminal damage).
- reduce fear of crime and antisocial behaviour.
- manage an exclusion scheme/list

We also use this data to identify natural persons for further action such as issuing exclusion notices to prevent and reduce crime and enhance local prosperity based on the national intelligence model.

Lawful basis for processing your data

We do not store, process, or share the data of persons on the exclusion list unless we have an appropriate lawful reason to do so.

Under Data Protection Legislation, the lawful bases we rely on for processing your information are:

- **GDPR, Article 6(1)(f) – We have a legitimate interest, namely to prevent and detect potential or actual criminal offences and anti-social behaviour in order to safeguard those persons who are out in the nighttime economy in Southampton.**

Additionally, where we may process any special category data we are required to identify an Article 9 lawful basis. For this our lawful basis will be:

- **Article 9 (2) (g) - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.**

Additionally, for both the Art 9 and Art 10 processing of criminal offence data, we are required to identify the substantial public interest condition that will be relied on as per Part 2 of Schedule 1 of the DPA 2018, which in this case is:

- **Preventing or detecting unlawful acts**

The Offenders on the exclusion list have been assessed to pose a significant enough threat to the safety of the people and property in the area that early, proactive identification and management of these persons, which may including barring them from entering and accessing certain locations and services, is the most appropriate course of action to take to prevent unlawful acts.

We may use your information for the following purposes:

Processing Activity	Lawful Basis
Prevent and detect potential crime or criminal offences	Legitimate Interest
Provide evidence to authorities for criminal investigations	Legitimate Interest
Add a person to the exclusion list	Legitimate Interest
Conduct internal regulatory or disciplinary investigations	Legitimate Interest
To respond to and defend against legal claims, where you have provided us with information which may give rise to legal claims	Legitimate Interest

We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Data without your knowledge or consent, in compliance with the above activities, or where this is required or permitted by law.

Who we might share your information with

We may share your personal data with:

- government bodies and regulatory authorities, including the Police and other crime prevention and detection agencies and the UK Information Commissioner’s Office;
- the courts and other dispute resolution arbitrators and mediators, other parties to legal proceedings; or
- If we need to share Personal Data in order to establish, exercise or defend our legal rights – this includes providing Personal Data to others for the purposes of detecting and preventing fraud.
- Other members of the Southampton Business Crime Partnership (SCBP).

We use Service Providers (“Data Processors”) who are third parties who provide elements of services for us. We have Data Processor Agreements in place with our data processors. This means that they cannot do anything with your Personal Data unless we have instructed them to do it. They will not share your Personal Data with any organisation apart from us or further sub-processors who must comply with our Data Processor Agreement. They will hold your Personal Data securely and retain it for the period we instruct.

Where we share your data with another data controller, we have entered into an appropriate data sharing agreement with them that governs the sharing of your data.

How long we keep your information for

We will always retain your Personal Data in accordance with the Data Protection Legislation and never retain your information for longer than is necessary. GO! Southampton has a retention schedule which outlines how long we will retain your Personal Data. As such, unless otherwise required by law, your data will be retained for the period specified below and then securely deleted in accordance with our internal policies and procedures.

- Minimum 12 months but may be for a period of up to 5 years (the maximum time a person can remain on the list)

When an offender is reported by a member for participating in any threat or damage to any member's property, staff or customers, his/her name and facial image may be shared among members for 12 months. If no further report is submitted during that period, the offender's data will be withdrawn from members at the expiry of that period. It will be retained for a further 12 months in the Scheme's database (which can only be accessed by the Data Controller) after which time it will be irrevocably deleted.

If during the 12 months when an offender's data is circulated among members, he/she is reported for another incident involving a threat or damage to any member's property, staff or customers, his/her name/ facial image and date of birth will be circulated among members for a further 24 months from the date of the second report. Additionally, the offender may be excluded from all the properties day or night-time, or both in some circumstances. The period for exclusion will be determined by the nature of the incident/s this can be anything from 6 months to 5 years and this fact will be shared with members. If no further report is submitted by a member during that period, the offender's data will be withdrawn from members at the expiry of that period. It will be retained for a further 12 months in the Scheme's database (which can only be accessed by the Data Controller) after which it will be deleted.

Your rights over your information

The right to be informed about our collection and use of personal data

You have the right to be informed about the collection and use of your personal data. We ensure we do this with our internal and external Privacy Notices (including this document). These are regularly reviewed and updated to ensure these are accurate and reflect our data processing activities.

Right to Access Your Personal Data

You have the right to access the Personal Data that we hold about you in many circumstances, by making a request. This is sometimes termed 'Data Subject Access Request.' If we agree that we are obliged to provide Personal Data to you (or someone else on your behalf), we will provide it to you or them free of charge and aim to do so within 1 month from when your identity has been confirmed.

We may ask for proof of identity and sufficient information about your interactions with us that we can locate your Personal Data.

If you would like to exercise this right, please **Contact Us** as set out below.

Right to Rectify Your Personal Data

If any of the Personal Data we hold about you is inaccurate, incomplete, or out of date, you may ask us to correct it.

If you would like to exercise this right, please **Contact Us** as set out below.

Right to Erasure

You have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances. For instance, the right to erasure does not apply where we have a legal obligation to retain your Personal Data.

If you would like to exercise this right, please **Contact Us** as set out below.

Right to Restrict Processing

You have the right to ask us to restrict the processing of your personal data. For example, this may be because you have issues with the accuracy of the data we hold or the way we have processed your data. The right is not absolute and only applies in certain circumstances.

If you would like to exercise this right, please **Contact Us** as set out below.

Right to Portability

The right to portability gives you the right to receive personal data you have provided to a controller in a structured, commonly used, and machine-readable format. It also gives them you the right to request that a controller transmits this data directly to another controller.

If you would like to exercise this right, please **Contact Us** as set out below.

Right to Object

You have the right to object to our processing of some or all the personal data that we hold about you. This is an absolute right if we use your data for direct marketing but may not apply in other circumstances where we have a compelling reason to do so, e.g., a legal obligation.

If you would like to exercise this right, please **Contact Us** as set out below.

Rights Related to Automated Decision-Making

You have the right to object to our processing where a decision is made about you solely based upon automated processes and which has significant or legal effects. However, this right does not apply as there is significant human involvement in decision making during the processing.

For more information about your privacy rights

In the UK, the Information Commissioner's Office (ICO) regulates data protection and privacy matters. They make a lot of information accessible to consumers on their website, which you can access here: <https://ico.org.uk/for-the-public>.

You can make a complaint to the ICO, or any other supervisory authority, at any time about the way we use your information. However, we hope that you would consider raising any issue or complaint you have with us first. We will always do our absolute best to solve any problems you may have.

Security

Data security is of great importance to GO! Southampton. We have put in place appropriate technical and organisational measures to prevent your Personal Data from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed.

We take security measures to protect your information including:

- Limiting access to our buildings and resources to only those that we have determined are entitled to be there;
- Managing a data security breach reporting and notification system which allows us to monitor and communicate information on data breaches with you or with the applicable regulator when required to do so by law;
- Implementing access controls to our information technology; and,

- Deploying appropriate procedures and technical security measures (including strict encryption, anonymisation and archiving techniques) to safeguard your information across all our computer systems, networks, websites, and offices.

International Transfers

It is not expected that we will transfer your personal data internationally.

However, if this does happen and we are required to transfer your Personal Data out of the UK or EU to countries not deemed by the ICO or European Commission (as relevant) to provide an adequate level of Personal Data protection, the transfer will be based on safeguards that allow us to conduct the transfer in accordance with the Data Protection Legislation, such as the specific contracts containing standard data protection clauses approved by the ICO or European Commission (as relevant) providing adequate protection of Personal Data. You can obtain a copy of this documentation by contacting us at **Contact Us** section below.

Contact Us

If you would like to exercise one of your rights as set out above, or you have a question or a complaint about this Privacy Notice or the way your Personal Data is processed, please contact our Data Protection Officer by one of the following means:

By email: stephen.manion@gosouthampton.co.uk

By post: Southampton Business Improvement District Ltd
Network Eagle Lab
Portland Terrace
Southampton
SO14 7SJ

Changes to Our Privacy Notice

Thank you for taking the time to read our Privacy Notice.

We may change this Privacy Notice from time to time (for example, if the law changes). We recommend that you check this Privacy Notice regularly to keep up to date.

This Notice was last updated March 2024