

How we use Personal Information

Introduction

This document explains how the States of Jersey Police (SOJP) obtains, holds, uses and discloses information about people - their personal information, the steps we take to ensure that it is protected, and also describes the rights individuals have in regard to their personal information handled by SOJP.

The use and disclosure of personal information is governed in Jersey by the Data Protection (Jersey) Law 2018 ('the Law'). SOJP's Chief Officer is registered with the Information Commissioner as a 'data controller' for the purposes of the Law. As such he is obliged to ensure that SOJP handles all personal information in accordance with the Law.

SOJP takes that responsibility very seriously and takes great care to ensure that personal information is handled appropriately in order to secure and maintain individuals' trust and confidence in the force.

1. Why do we handle personal information?

SOJP obtains, holds, uses and discloses personal information for two broad purposes:

1. The Policing Purpose – which includes the prevention and detection of crime; apprehension and prosecution of offenders; protecting life and property; preserving order; maintenance of law and order; rendering assistance to the public in accordance with force policies and procedures; and any duty or responsibility of the police arising from common or statute law.
2. The provision of services to support the Policing Purpose – which include:
 - Staff administration, occupational health and welfare
 - Management of public relations, journalism, advertising and media
 - Management of finance
 - Internal review, accounting and auditing
 - Training
 - Property management
 - Insurance management
 - Vehicle and transport management
 - Payroll and benefits management
 - Management of complaints
 - Vetting

1 'Personal Data' is defined under Article 2 of the Data Protection (Jersey) Law 2018. In practical terms it means information handled by SOJP that relates to identifiable living individuals. It can include intentions and expressions of opinion about the individual. The information can be held electronically or as part of paper records, and can include CCTV footage and photographs. For ease of readers this document refers to the handling, use, holding etc. of personal data – Article 1 of the Law uses the term 'processing' to effectively cover any usage of personal data.

2 This document is designed to help satisfy the 'Fair Processing Requirements' as required by Article 12 of the Data Protection (Jersey) Law 2018 and may be regarded as a generic over-arching 'Fair Processing Notice' for SOJP. Additional more specific Fair Processing Notices may appear in other circumstances such as on forms, force policies, email footers, or CCTV signage.

- Management of information technology systems
- Legal services
- Information provision
- Licensing and registration
- Pensioner administration
- Research, including surveys
- Performance management
- Sports and recreation
- Procurement
- Planning
- System testing
- Security
- Health and safety management

2. Whose personal information do we handle?

In order to carry out the purposes described under section 1 above, SOJP may obtain, use and disclose (see section 7 below) personal information relating to a wide variety of individuals including the following:

- Staff including volunteers, agents, temporary and casual workers
- Suppliers
- Complainants, correspondents and enquirers
- Relatives, guardians and associates of the individual concerned
- Advisers, consultants and other professional experts
- Offenders and suspected offenders
- Witnesses
- Victims
- Former and potential members of staff, pensioners and beneficiaries
- Other individuals necessarily identified in the course of police enquiries and activity

SOJP will only use appropriate personal information necessary to fulfil a particular purpose or purposes. Personal information could be information which is held on a computer, in a paper record such as a file, as images, but it can also include other types of electronically held information such as CCTV images.

3. What types of personal information do we handle?

In order to carry out the purposes described under section 1 above, SOJP may obtain, use and disclose (see section 7 below) personal information relating to or consisting of the following:

- Personal details such as name, address, biographical details
- IP address, vehicle registration
- Family, lifestyle and social circumstances
- Education and training details
- Employment details
- Financial details

3 SOJP regularly conducts Customer Satisfaction Surveys to evaluate our performance and effectiveness. We may contact individuals, such as victims of crime or those reporting incidents, and ask them to give us their opinion of the service we are providing to the public. We use the information given to improve our service wherever we can. SOJP, like many police forces sometimes uses a private company to undertake such surveys on our behalf with strict controls to protect the personal data of those involved.

- Goods or services provided
- Racial or ethnic origin
- Political opinions
- Religious or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Offences (including alleged offences)
- Criminal proceedings, outcomes and sentences
- Biometric identifiers including DNA, fingerprints, photographs and other genetic samples
- CCTV including sound and visual images
- Licenses or permits held
- Criminal Intelligence
- References to manual records or files
- Information relating to health and safety
- Complaint, incident and accident details

4. Where do we obtain personal information from?

In order to carry out the purposes described under section 1 above SOJP may obtain personal information from a wide variety of sources, including the following:

- Other law enforcement agencies
- The Honorary Police
- Jersey Customs and Immigration HM Revenue and Customs
- International law enforcement agencies and bodies
- Licensing authorities
- Legal representatives
- Prosecuting authorities
- Defence advocates or solicitors
- Courts
- Prisons
- Security companies
- Partner agencies involved in crime and disorder strategies
- Private sector organisations working with the police in anti-crime strategies
- Voluntary sector organisations
- Approved organisations and people working with the police
- Jersey Police Complaints Authority
- Her Majesty's Inspectorate of Constabulary
- Auditors
- Police Authorities
- Central government, governmental agencies and departments
- Emergency services
- Individuals themselves
- Relatives, guardians or other persons associated with the individual
- Current, past or prospective employers of the individual
- Healthcare, social and welfare advisers or practitioners
- Education, training establishments and examining bodies
- Business associates and other professional advisors
- Employees and agents of SOJP

- Suppliers, providers of goods or services
- Persons making an enquiry or complaint
- Financial organisations and advisors
- Credit reference agencies
- Survey and research organisations
- Trade, employer associations and professional bodies
- The Parishes
- Voluntary and charitable organisations
- Ombudsmen and regulatory authorities
- The media
- Data processors working on behalf of SOJP

5. How do we handle personal information?

In order to achieve the purposes described under section 1 SOJP will handle personal information in accordance with the Law. In particular we will ensure that personal information is handled fairly and lawfully with appropriate justification. We will strive to ensure that any personal information used by us or on our behalf is of the highest quality in terms of accuracy, relevance, adequacy and non-excessiveness, is kept as up-to-date as required, is protected appropriately, and is reviewed, retained and securely destroyed when no longer required. We will also respect individuals' rights under the Law (see section 8 below).

6. How do we ensure the security of personal information?

SOJP takes the security of all personal information under our control very seriously. We will comply with the relevant parts of the Law relating to security, and seek to comply with the College of Policing guidelines for Information Assurance which is available at <https://www.app.college.police.uk/app-content/information-management/information-assurance/> and relevant parts of the ISO27001/2 Information Security Standard.

We will ensure that appropriate policy, training, technical and procedural measures are in place, including audit and inspection, to protect our manual and electronic information systems from data loss and misuse, and only permit access to them when there is a legitimate reason to do so, and then under strict guidelines as to what use may be made of any personal information contained within them. These procedures are continuously managed and enhanced to ensure up-to-date security.

7. Who do we disclose personal information to?

In order to carry out the purposes described under section 1 above SOJP may disclose personal information to a wide variety of recipients in any part of the world, including those from whom personal information is obtained (as listed above). This may include disclosures to other law enforcement agencies, partner agencies working on crime reduction initiatives, partners in the Criminal Justice arena, Victim Support, and to bodies or individuals working on our behalf such as IT contractors or survey organisations. We may also disclose to other bodies or individuals where necessary to prevent harm to individuals.

Where required, or appropriate to do so, personal data may be shared with the office of the Jersey Police Authority to facilitate and support policing and to deliver applicable statutory functions. Disclosures of personal information will be made on a case-by-case basis, using the personal information appropriate to a specific purpose and circumstances, and with necessary controls in place.

Some of the bodies or individuals to which we may disclose personal information are situated outside of the European Union - some of which do not have laws that protect data protection rights as extensively as in Jersey. If we do transfer personal information to such territories, we will take proper steps to ensure that it is adequately protected as required by the Law.

SOJP will also disclose personal information to other bodies or individuals when required to do so by any rule of law, and by court order. SOJP may also disclose personal information on a discretionary basis for the purpose of, and in connection with, any legal proceedings or for obtaining legal advice.

8. What are the rights of the individuals whose personal information is handled by SOJP?

Individuals have various rights enshrined in the Law:

Subject Access

The most commonly exercised right is that used by individuals to obtain details, subject to exemptions, of their personal information processed by SOJP. Details of the application process, known as 'Subject Access' can be found from the force internet at:

<https://jersey.police.uk/accessing-information/personal-information-access/>

Alternatively individuals may contact the SOJP Data Protection Officer (see section 11 below).

Right to withdraw consent

If we are relying on your consent to process your personal data, it must be freely given, informed and unambiguous, and you may change your mind at any time. You cannot consent to the processing of your personal data if you are a child under 13 years of age; however a person with parental responsibility may do so on your behalf.

Right to restriction of processing

Under Article 33 of the Law an individual is entitled, in limited circumstances, to write to SOJP requesting a restriction on processing, such as where the accuracy of their personal data is contested. All requests of this nature may be sent in writing to the Force Data Protection Officer (see section 11 below). It is worth noting that the Law includes certain provisions which may mean in a particular case that SOJP can continue to handle the personal data as intended despite the objection.

Right to Prevent Processing for the Purposes of Direct Marketing

Although SOJP does not engage in direct-marketing, under Article 36 of the Law, and NOT subject to certain exemptions, an individual has the right to request in writing that SOJP stops within a reasonable time, or does not start, using their personal information for direct marketing purposes. This includes the communication by any means (e.g. mail, email, telephone, door-to-door canvassing) of any advertising or marketing material directed at particular individuals.

Any requests under Article 36 may be sent to the Force Data Protection Officer (see section 11 below).

Rights in relation to automated decision-taking

In circumstances where processing of personal data has been inactive for a significant period of time and where it is no longer necessary or proportionate to hold, the data may be automatically deleted without any human intervention.

Under certain conditions, Article 38 of the Law gives an individual the right to ensure that no decision that would significantly affect them is taken by SOJP or on its behalf purely using automated decision-making software. If there is any human element involved in the decision-making the right does not apply. Requests under Article 38 may be sent to our Data Protection Officer (see section 11 below).

Right to take action for compensation if the individual suffers damage by any contravention of the Law by data controllers

Under Article 68 of the Law any individual who believes they have suffered loss, damage or distress as a result of any contravention of the requirements of the Law may be entitled to compensation from SOJP where we are unable to prove that we had taken such care as was reasonable in all the circumstances to comply with the relevant requirement. Any claim for compensation arising from this provision may be sent to:

The Chief Officer,
States of Jersey Police,
Police Headquarters,
La Route du Fort,
St Helier,
Jersey, JE2 4PA

Right to rectification of inaccurate or incomplete data

Under certain conditions, Article 31 of the Law gives an individual the right to request SOJP to rectify inaccurate or incomplete personal information. We would also need to inform other data controllers if we have shared inaccurate or incomplete data with them. Requests under Article 31 may be sent to our Data Protection Officer (see section 11 below).

Right to erasure

Under certain conditions, Article 32 of the Law gives an individual the right to request SOJP to erase personal information where our processing breaches any of the data protection principles. If this were to be the case, we would also need to consider informing other data controllers who may be processing this information. Requests under Article 32 may be sent to our Data Protection Officer (see section 11 below).

Right to portability

Under certain very limited conditions, Article 34 of the Law gives an individual the right to request SOJP to provide their personal data in a structured, commonly used and machine readable format, and to transfer their personal data to another data controller. We do not have to comply with such a request if we are processing such information for law enforcement work (which is the majority of our business activity), or where it would adversely affect the rights and freedoms of others. Requests under Article 34 may be sent to our Data Protection Officer (see section 11 below).

Right to object to processing for purpose of public functions

Under certain conditions, Article 35 of the Law gives an individual the right to object to the processing of their personal data where the “public functions” condition has been exclusively relied upon. We would not have to stop processing personal data if we can show that the public interest to do so either outweighs the individual’s interests, rights and freedoms, or is necessary for the establishment, exercise or defence of legal claims. Requests under Article 35 may be sent to our Data Protection Officer (see section 11 below).

Right to request the Information Commissioner to assess a data controller’s Processing

Under Article 19 of the Data Protection Authority (Jersey) Law 2018 any person can make a complaint to the Information Commissioner if they believe that they are/have been adversely affected by the handling of personal data by SOJP. Such requests should be made direct to the Information Commissioner whose contact details can be found below.

Generally if individuals have any concerns regarding the way their personal data is handled by SOJP or the quality (accuracy, relevance, non-excessiveness etc.) of their personal data, they are encouraged to raise them with the Force Data Protection Officer in the first instance (see section 10 below).

The Information Commissioner is the independent regulator responsible for enforcing the Law and can provide useful information about the Law's requirements.

The Information Commissioner may be contacted using the following:

The Office of the Information Commissioner Brunel House,
Old Street,
St Helier,
Jersey, JE2 3RG
Telephone: 01534 716530
Email: enquiries@oicjersey.org
Website: www.oicjersey.org/

9. How long does SOJP retain personal information?

SOJP keeps personal information as long as is necessary for the particular purpose or purposes for which it is held. In respect of the Police National Computer (PNC), personal information is retained, reviewed and deleted in accordance with agreed national retention periods which are subject to periodic change. Records containing personal information relating to intelligence, custody, crime, firearms, conviction history, child abuse investigations, and domestic violence will be retained in accordance with national police policy, which is the Guidance on the Management of Police Information (MoPI) 2010. This can also be found on the College of Policing (NPIA) website: <http://www.app.college.police.uk/app-content/information-management/management-of-police-information/>

10. Monitoring

SOJP may monitor or record and retain telephone calls, texts, emails and other electronic communications to and from the force in order to deter, prevent and detect inappropriate or criminal activity, to ensure security, and to assist the purposes described under section 1 above.

11. Contact Us

Any individual with concerns over the way SOJP handles their personal information may contact our Data Protection Officer as below:

Data Protection Officer,
States of Jersey Police,
La Route du Fort,
St Helier,
Jersey, JE2 4HQ
Telephone: 01534 612612
Email: enquiries@oicjersey.org
Website: www.jersey.police.uk