Data Protection From First Principles

Lawful Bases For Processing

Presented by

Huw Thomas

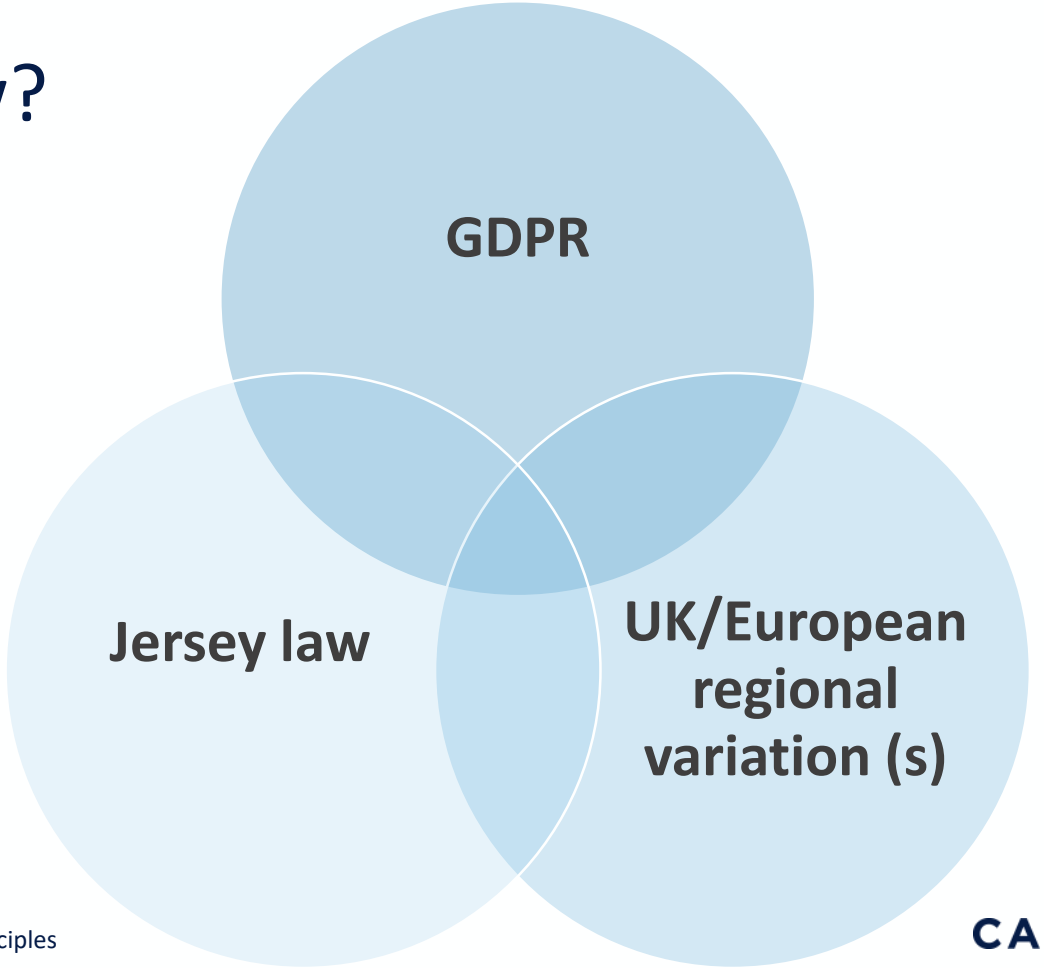
Counsel, Jersey

16 March 2018

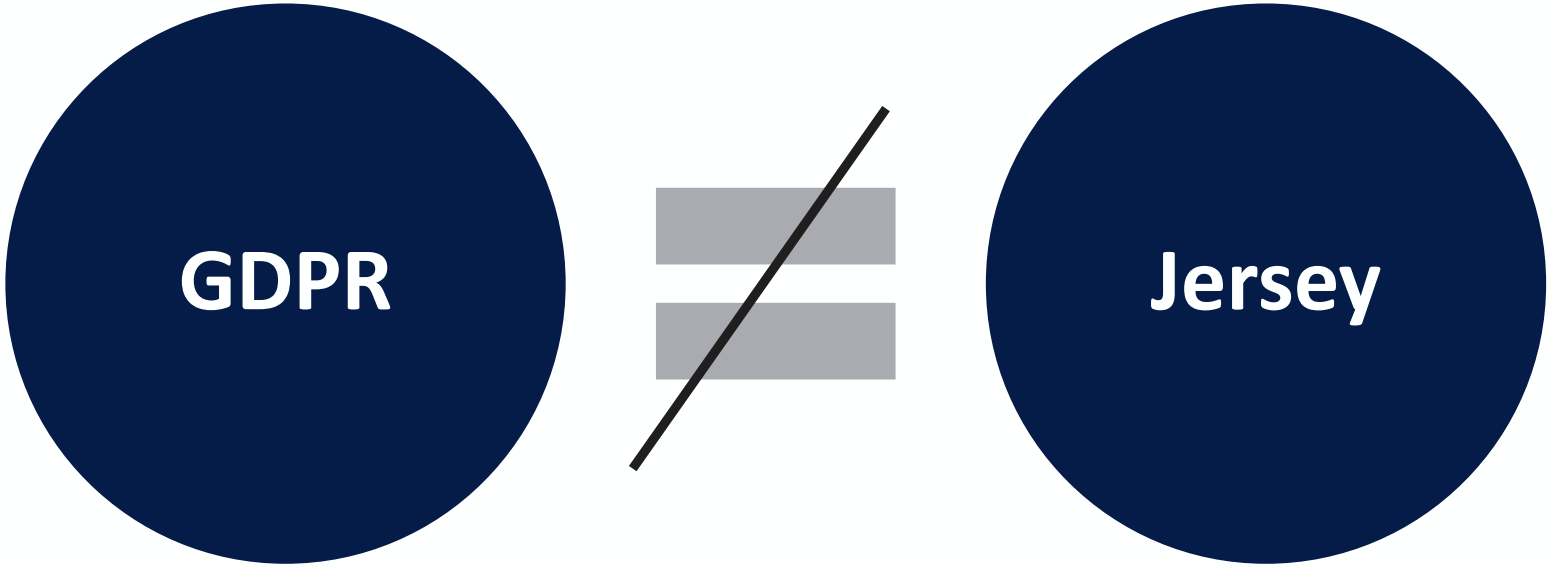
J.DPA
JERSEY DATA PROTECTION ASSOCIATION

CAREY OLSEN

Which Law?



Law Basis for Processing



What’s personal data?

“**Personal data**" means any information relating to an identified or identifiable natural person (a '**data subject**')

What's personal data?

- **'Any information**' is understood to be literal. Information could be anything from a person's name to her location.
- **'Relating to**' refers to the information's purpose and impact on someone's privacy rights. Its juxtaposition with other content is also important. For example, a job title would not necessarily relate to a person, but a job title combined with a name likely would.
- '**Identified**' means that an individual person has been named or singled out—for example, by specific characteristics. 'Identifiable' includes **indirect identification**, taking into account all the 'means reasonably likely to be used' to identify the person.
- A **'natural person**' is a real human being, as distinguished from a corporation. This person is referred to as the **data subject**.

Sensitive/Special Category Personal Data

Expanded Definition

- Personal data revealing racial or ethnic origin
- Political opinions,
- Religious or philosophical beliefs, or
- Trade-union membership;
- Genetic or biometric data for the purpose of uniquely identifying a natural person; and
- Data concerning health, sex life or sexual orientation
- [**Jersey - data relating to a natural person's criminal record or alleged criminal activity]**

Preconditions to Law Processing

- DPJL Article 6(1)(b)/22(1)(a) – controllers and processors (if established in Jersey), may cause or permit personal data to be processed only if the processor meets the requirement to be registered
- Transitional arrangements – current registration approach will continue up to no later than 25 May 2019
- Intention then is to have a tiered risk based fee structure

Law Basis for Processing – Why It's Important

Lawful Processing – Applicable Principles

Art 5(a) GDPR/8(1)(a) DPJL –

Lawfulness, fairness and transparency

- Personal data shall be processed **lawfully**, **fairly** and in a **transparent** manner in relation to the data subject

Art 5(2) GDPR/6(1) DPJL –

Accountability

- The controller shall be **responsible** for, and **be able to demonstrate compliance** with the the principles

Demonstrating Compliance with the Law

Article 24 GDPR/24 DPJL

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Privacy Notices

Article 13/14 GDPR/12 DPJL

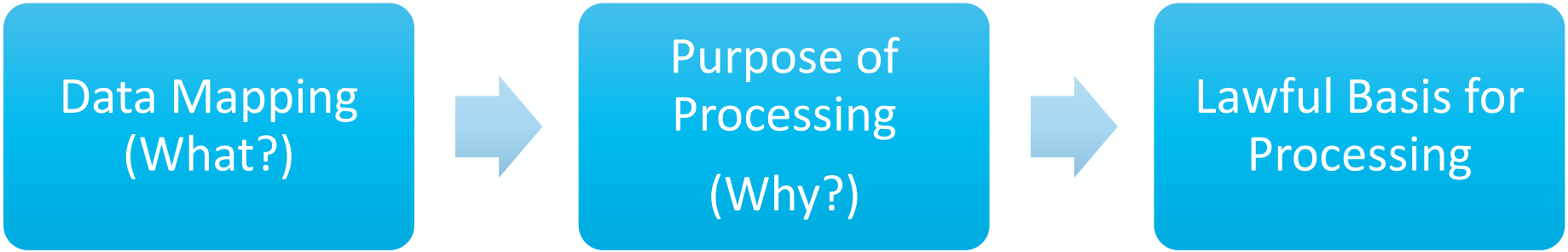
Privacy Notices must include:

- the purposes for which the data are intended to be processed and the **legal basis** for the processing; and
- an explanation of the **legitimate interests** pursued by the controller or by a third party, if the processing is based on those interests.

Impact on Individual Rights

- The right to erasure does not apply to processing on the basis of legal obligation or the exercise of public authority (Article 17(3)(b) GDPR/32(3)(b) DPJL).
- The right to portability only applies to processing on the basis of consent or contract (Article 20(1) GDPR/34(2) DPJL).
- The right to object only applies to processing on the basis of public functions or legitimate interests (Article 21(1) GDPR/35(1) DPJL).

Lawful Processing – where it fits in

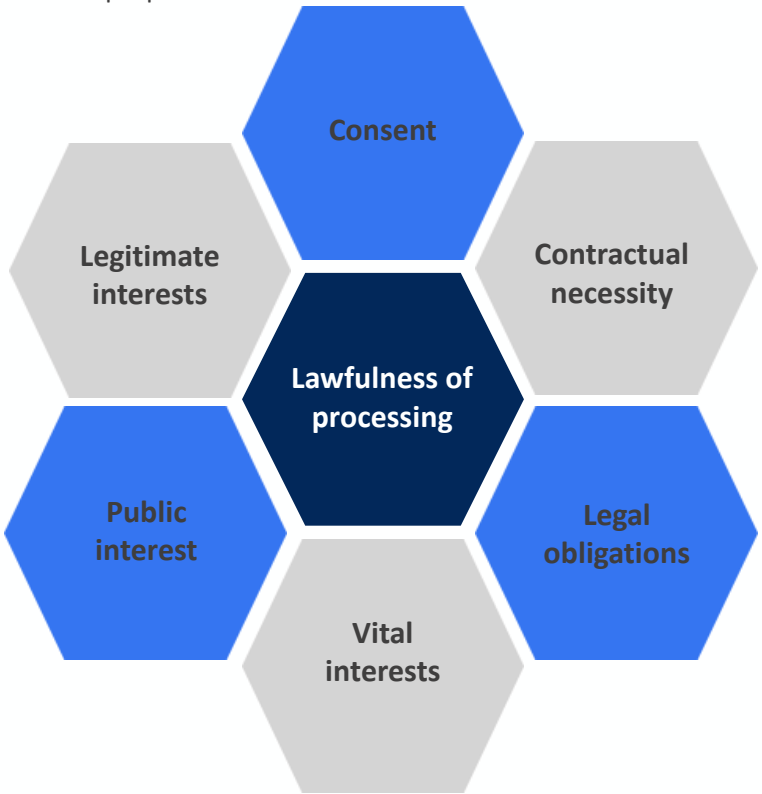


The GDPR

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Consent

Individual has given clear consent for you to process their personal data for a specific purpose



Legitimate interests

Processing is necessary for your (or someone else's legitimate interests unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Public interest

Public authorities and organisations in the scope of public duties and interest

Contractual necessity

Processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

Legal obligations

You are obliged to process personal data for a legal obligation

Vital interests

Processing is necessary to protect someone's life

“Necessary”

- Does not mean that processing always has to be **essential**.
- Must be a **targeted** and **proportionate** way of achieving the purpose.
- Does not = necessity not apply if you can reasonably achieve the purpose by some other less intrusive means.

ICO Guidance - *It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.*

Consent

(Article 7 GDPR/11 DPJL)

11 Consent to processing

(1) In this Law, "consent", in relation to the processing of a data subject's personal data, means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, whether orally or in writing, signifies agreement to the processing of that data.

Consent

(Article 7 GDPR/11 DPJL)

Unbundled: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

Active opt-in: pre-ticked opt-in boxes are invalid – use unticked opt- in boxes or similar active opt-in methods (eg a binary choice given equal prominence).

Granular: give granular options to consent separately to different types of processing wherever appropriate.

Named: name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.

Consent

Documented: keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.

Easy to withdraw: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place.

No imbalance in the relationship: consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis.

Necessary for the Performance of a Contract

Article 6(1)(b) GDPR/Schedule 2 Part 1 Paragraph 1

The processing is necessary for –

- the performance of a contract to which the data subject is a party; or
- the taking of steps at the request of the data subject with a view to entering into a contract.

Legal Obligation

Article 6(1)(c) GDPR/Schedule 2 Part 2 DPJL

Compliance with a legal obligation to which the controller is subject

GDPR – basis for processing must be laid down in **Union/Member State Law**

Narrow construction? GDPR applies to legal obligations required by EU and member state laws only. It does not include legal obligations of contracts or those of third countries (outside the EU).

Open to question as to status of laws of “adequate jurisdictions”

WP29 Swift Opinion

It is also important to emphasise that Article 7(c) refers to the laws of the European Union or of a Member State. Obligations under the laws of third countries (such as, for example, the obligation to set up whistleblowing schemes under the Sarbanes–Oxley Act of 2002 in the United States) are not covered by this ground. To be valid, a legal obligation of a third country would need to be officially recognised and integrated in the legal order of the Member State concerned, for instance under the form of an international agreement. On the other hand, the need to comply with a foreign obligation may represent a ***legitimate interest of the controller****, but only subject to the balancing test of Article 7(f), and provided that adequate safeguards are put in place such as those approved by the competent data protection authority.*

Vital Interests

Article 6(1)(d) GDPR/Schedule 2 Part 2 Para 9 DPJL

The processing is necessary in order to protect the vital interests of –

- the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the controller cannot reasonably be expected to obtain the consent of the data subject; or
- another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

Public Interest/Official Authority

Article 6(1)(e) GDPR/Schedule 1 Part 1 Para 4 DPJL

- You can rely on this lawful basis if you need to process personal data:
  - 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
  - to perform a specific task in the public interest that is set out in law.
- It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.

.

Public Interest/Official Authority

- The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.
- Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis

Legitimate Interests

Article 6(1)(f) GDPR/Schedule 1 Part 1 Para 5 DPJL

5 Legitimate interests

(1) The processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, unless –

(a) the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject, in particular where the subject is a child; or

(b) the controller is a public authority

Legitimate Interests

- **Purpose test:** are you pursuing a legitimate interest?
- **Necessity test:** is the processing necessary for that purpose?
- **Balancing test:** do the individual's interests override the legitimate interest?

Legitimate Interests

GDPR suggests some potential examples of legitimate interests:

- client or employee data
- Direct marketing (if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object)
- fraud prevention
- intra-group transfers; or
- IT security as potential legitimate interests

ICO Guidance

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interests assessment (LIA) and you should do it before you start the processing.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

Conditions for Processing Special Categories

GDPR

- Explicit consent
- In the context of employment
- Vital interests (controller must be able to demonstrate that it is not possible to obtain consent).
- Political, philosophical and religious purposes: This criterion covers particular (foundations, associations, not-for-profit bodies and any foundation, association or not-for-profit body with trade union aims)
- Data made public by data subject
- Necessary for the establishment, exercise or defence of legal claims
- Substantial public interest
- Preventive or occupational medicine
- Public health

CAREY OLSEN

Criminal Records

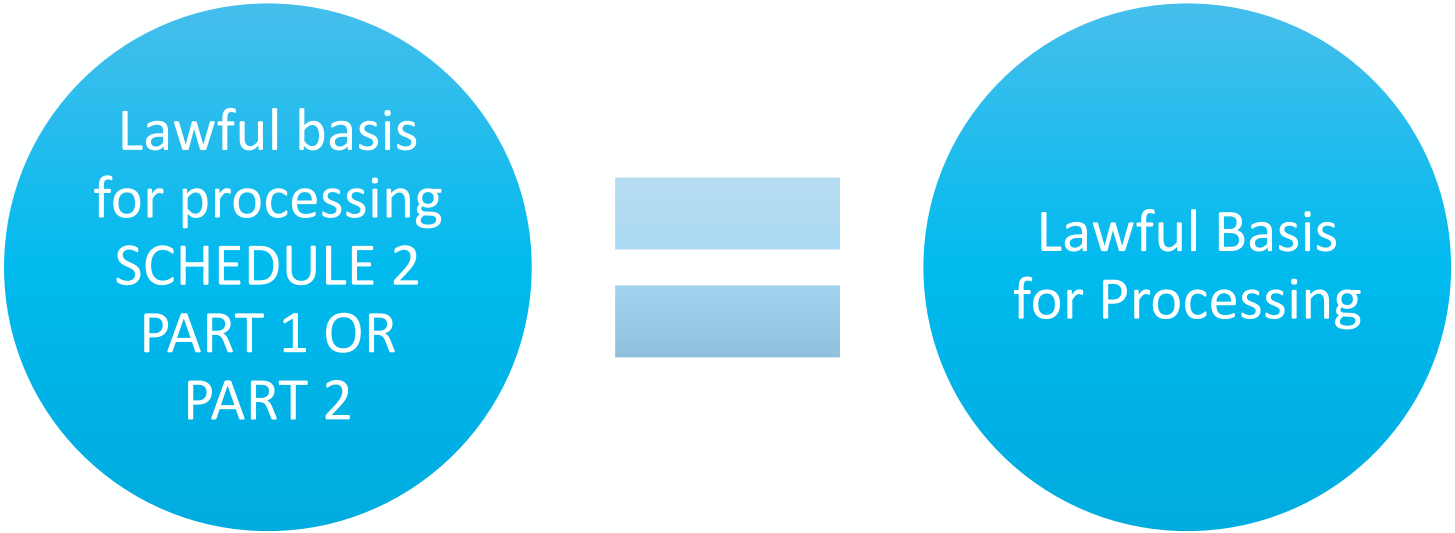
- GDPR - Specific regime – only where legally authorised
- Art 42 DPJL –

Despite anything to the contrary in this Law a person may require another person to provide any criminal record certificate that may lawfully be obtained by, or in relation to, the data subject under any provision of the Police Act 1997 of the United Kingdom as it extends to Jersey.

GDPR – Cumulative

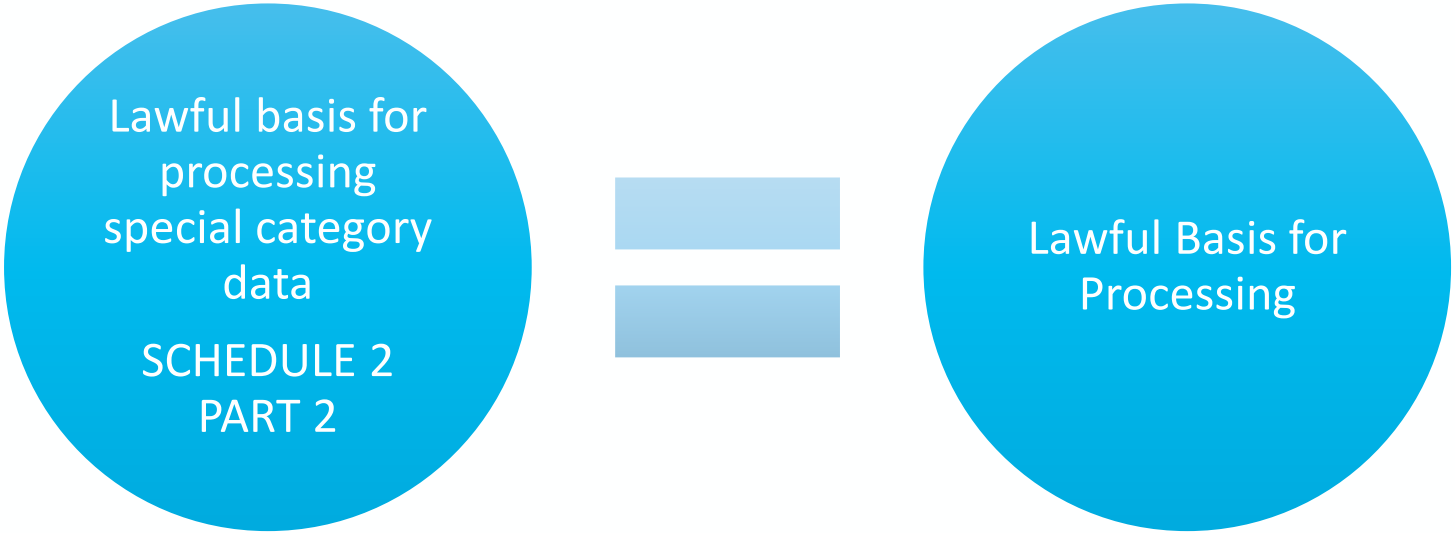
DPJL– ONE STEP

PERSONAL DATA



DPJL– ONE STEP

SPECIAL CATEGORIES OF DATA



DPJL

SCHEDULE 2 PART 1 – PERSONAL DATA

- Consent
- Contract
- Vital interests
- Public functions
- Legitimate interests

DPJL

SCHEDULE 2 PART 2

- Consent
- Other legal obligations
- Employment and social fields
- Vital interests of data subject or another
- Non-profit associations
- Information made public by data subject
- Legal proceedings, etc.
- Public functions/Public interest
- Medical purposes (includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment, the management of healthcare services, occupational medicine and the assessment of the working capacity of the employee.)
- Public health
- Archiving and research

DPJL

SCHEDULE 2 PART 2

- Archiving and research
- Avoidance of discrimination
- Prevention of unlawful acts
- Protection against malpractice and mismanagement
- Publication about malpractice and mismanagement
- Counselling
- Insurance and pensions: general determinations
- Insurance and pensions: current processing
- Functions of a police officer
- Regulations

Why change?

"What Orwell failed to predict was that we'd buy the cameras ourselves and that our biggest fear would be that no-one was watching."

(Keith Lowell Jensen)

Questions

J.DPA
JERSEY DATA PROTECTION ASSOCIATION

CAREY OLSEN

Guidance

www.ico.org

www.thinkgdpr.org

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

https://dataprotection.ie/

https://jdpa.org.je/

Contact details

Huw Thomas

Counsel, Jersey

D +44 (0)1534 822224

E huw.thomas@careyolsen.com