compliant • commercial • creative

DATA PROTECTION

The Data Protection (Jersey) Law 2018 grants people a range of specific rights they can exercise over their personal data, in certain circumstances (exemptions may apply). It also sets out the requirements for how organisations, businesses and the government use your personal information.

What you need to know…

- Data Subject: the individual whose data is being held and processed
- Data Controller: determines the purposes and means of processing personal data
- Data Processor: is responsible for processing personal data on behalf of a controller

More definitions can be obtained from the JOIC by clicking here

DATA PROTECTION PRINCIPLES

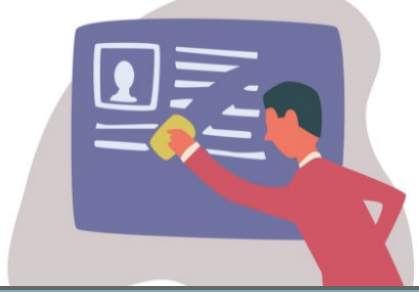
Data Processors and Data Controllers must follow these principles:

1. Used lawfully, fairly and transparently
2. Used for specified, explicit and legitimate purposes
3. Used in a way that is adequate, relevant and limited to only what is necessary
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary
6. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

SENSITIVE DATA

There is stronger legal protection for sensitive information which is also known as special category data, such as: Race, Ethnic Background, Political Opinions, Religious Beliefs, Trade Union Membership, Genetics or Biometrics (where used for identification), Health, Sex Life or Orientation, Criminal Record or Alleged Criminal Activity.

INDIVIDUAL RIGHTS



Individual rights include the rights to:

- Be informed about how your data is being used.
- Access personal data.
- Have incorrect data updated.
- Have data deleted (in certain circumstances).
- Limit or restrict the processing of your data (in certain circumstances).
- Data portability (allowing individuals to obtain and reuse your data for different services).
- Object to how your data is processed (in certain circumstances).

- Anyone can put in a SAR and there is no charge. It must be in writing.
- SARS must be responded to within 4 weeks. In complex cases, you may be able to apply for an extension.
- The individual should specify exactly what information or processing activities their request relates to. If not, seek clarification.
- If they request the SAR electronically, respond to them in a commonly used electronic form, unless the individual requests otherwise.
- If a Company does not comply, they may be faced with a fine.
- Redact names where correspondence contains personal data relating to others.

SUBJECT ACCESS REQUEST (SAR)

What you need to do…

EMPLOYER'S PERSPECTIVE
CONSIDERATIONS WHEN WORKING AWAY FROM THE OFFICE

- Make sure you have a SAR policy that everyone can access.
- Data must be organised, saved and destroyed in line with the retention and privacy policy.
- Train employees on Data Protection and remind them of their duties regularly.
- Make sure you have employees' consent on what data you keep and how you process it.
- Make sure employees are aware of the data privacy and confidentiality policies.
- Ensure retention policies are adhered to, even when working remotely.
- Provide work laptops and phones with the correct security enabled features, rather than employees using their own devices.
- Have a clear remote working policy that covers any data protection policies.
- Consider logging / restricting what documents leave the office or are downloaded from devices.

EMPLOYEE'S PERSPECTIVE
CONSIDERATIONS WHEN WORKING REMOTELY

- Ensure personal data is secure; at home it must be secure and your PC / laptop should be locked when you are not working at it.
- Be careful who is listening, switch off Alexa!
- Don't put anything into an email that you send from home, that you wouldn't include in an email sent from the office – remember all systems are trackable and discoverable in a SAR.
- Keep all paperwork in a secure way and shred it when back in the office.
- Use secure WiFi.
- Use only appropriate and approved software.
- Lock information away so members of the household cannot see it.
- Do not share comments about people, even if Covid-19 is confirmed or suspected (medical conditions are classed as sensitive data and should never be discussed).

REMEMBER!!

- Data protection principles apply wherever you work.
- Have a clear Data Protection policy in place and refresh.
- Train employees regularly on what is acceptable and any new updates.
- Don't ignore SARs, action them immediately.