Data Protection
Basic compliance guide

information commissioner
Barrantagh Fysseree

'Data protection' is about handling information about people, such as customers, clients and employees, in a way that is open, transparent, secure and fit for the digital era. Meeting their expectations will enhance the level of trust and confidence they have in an organisation and good information governance may save both time and money.

Fundamental definitions

- Information about living individuals (for example, staff, customers, volunteers, club members, potential clients, or members of the public) is **'personal data'**.
- Collecting, storing, recording and using personal data either electronically or in hardcopy is **'processing'**.
- Any type of organisation, such as a business, company, charity, club, association, online retailer, sole trader, etc. that decides what personal data is needed to operate or provide the service, why, and how it is processed, is the '**controller'**.
- Another organisation or company that the controller engages to provide particular services which involve the processing of personal data, such as direct marketing, accounting, payroll provision, recruitment, research, IT provision, is a **'processor'**.

Who must comply?

All **controllers** must comply with the law - it does not matter how big or small the controller is, what the controller does, or how many staff, customers or clients, etc. it has.

(**Processors** have particular obligations under the new law which are not covered in this guide. *Find out more: https://www.inforights.im/organisations/data-protection-law-2018/controllers-and-processors/processors/)*

How to comply

In order to comply with the law, controllers must understand and demonstrate:

- Why they legitimately use personal data (the purposes) and how it flows in and out;
- What the minimum necessary personal data needed to fulfil each of those different purposes is, and how it is kept accurate and up-to-date;
- Whether any personal data is disclosed to named third parties, and in what circumstances;
- What security measures are needed to protect the personal data (this may vary depending on the particular purpose and what type of personal data is being processed);
- How long that personal data must be kept for the particular purpose.

In summary, this is known as **'complying with the principles'**.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/principles-of-data-protection/

Controllers are **accountable for and must be able to demonstrate, compliance**. Some form of record showing how they comply should be kept and reviewed and updated as necessary. There is no standard format but the record should be understandable to the controller and as simple or

complex as needed.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/accountability-and-governance/records-of-processing-activities/

Such a record will also help controllers comply with their other obligations including **complying with the rights of individuals**, such as the right of access, the right to erasure and the right to object.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/rights/

Transparency (fair processing notices)

Individuals have a right to be given **information about the use of their personal data** and most of the information required for fair processing notices can be found in the details the controller has recorded about the processing being undertaken.

Controllers must give this information to individuals in clear, concise and plain language and it must contain details of their rights, including the right to complain to the Commissioner.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/rights/information-about-processing/

Registration

Registration is a component of compliance and controllers must register if:

- Personal data is automatically processed by the controller (or on its behalf by a processor); and
- The purposes for that processing are for **more than just**:
    - Administering its own staff;
    - Managing its own accounts.

Examples of where registration **is** required include:

- Installation of CCTV or use of other surveillance equipment, such as body-worn cameras, dash-cams, vehicle tracking
- Use of electronic communications for direct marketing to individuals (Email/SMS etc)
- Anti money-laundering obligations

The controller, having established the purposes for processing personal data, will know whether registration is required. In most cases controllers will need to register and a fee is usually payable.

Find out more, including whether a fee is payable: https://www.inforights.im/registration/

FAQs

Why bother complying?

The level of trust and confidence in your organisation depends on the integrity you show in handling your clients' personal information. Your own expectations of privacy should inform your practices in creating a culture of respect for your clients' personal information and a holistic approach to handling it in a way that is open, transparent, secure and fit for the digital era.

It is also the law – failure to comply with the law, and be accountable for compliance, may result in a loss of business or clientele, enforcement action or penalties imposed by the Commissioner, court imposed fines and awards of compensation. There are also criminal offences, some of which include terms of imprisonment.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/offences-sanctions-and-penalties/

I don't do any of the processing - am I still a controller?

The controller makes the decision about what personal data is needed to provide its services, pay staff etc., and how that processing is undertaken - it doesn't matter whether it does the physical processing itself or not.

> *For example: a repair company will need the names and addresses of its customers in order to send invoices, but may engage an accountant (a processor) to do that activity on its behalf. The repair company is still the controller as it has decided what personal data is needed and how it is to be processed.*

Where other laws mandate that certain personal data must be processed, this automatically makes the organisation which is subject to that law a controller, even if it outsources its compliance with that obligation to a third party.

> *For example, employment law requires an employer to give employees a written itemised pay statement. Although this function may be outsourced to a payroll administration company (a processor), the employer is still the controller.*

What if it goes wrong?

You must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk the processing poses to an individual, particularly the risk caused by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data that you process.

If you get a personal data breach, you must:

- take steps to investigate
- record the incident, including the facts, the effects and any remedial action taken
- inform the Commissioner within 72 hours of becoming aware, unless the personal data breach is unlikely to result in **any risk to the rights and freedoms of individuals**

- inform the individuals if it is likely that the breach will result in a high risk to their rights and freedoms

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/personal-data-breach/

Can individuals complain?

Yes – individuals are entitled to complain to the Commissioner about how you have handled their personal data and if you have not complied with their rights.

The Commissioner must investigate complaints and can take enforcement action or, if necessary, impose a financial penalty. You are required to co-operate with the Commissioner.

Individuals can also take action against the controller in court and seek compensation.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/remedies-for-individuals/

Do I always need consent for processing?

No – consent is only one of the 6 different lawful grounds for processing. Any one of the others may be more appropriate depending on the circumstances.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/principles-of-data-protection/lawfulness-fairness-and-transparency/lawfulness/

And https://www.inforights.im/organisations/data-protection-law-2018/principles-of-data-protection/lawfulness-fairness-and-transparency/lawfulness/consent/

Can I send direct marketing?

It is a legitimate interest of controllers to advertise and market their own goods and services. However, as most direct marketing is now by electronic means, e.g. SMS or email, you must therefore comply with the Unsolicited Communications Regulations.

Find out more: https://www.inforights.im/organisations/direct-marketing/guidance-for-marketers/

Do we need a Data Protection Officer?

A nominated Data Protection Officer will be needed in specific circumstances and the name of that person must be communicated to the Commissioner.

Find out more: https://www.inforights.im/organisations/data-protection-law-2018/data-protection-officers/

Other guidance available:

https://www.inforights.im/organisations/data-protection-law-2018/
https://www.inforights.im/media/1784/2020-small-business-compliance-guide.pdf
https://ico.org.uk/for-organisations/making-data-protection-your-business/does-data-protection-law-apply-to-my-business/