15 May 2018

Overall rating

Your overall rating was green.

- 0: Not yet implemented or planned
- 7: Partially implemented or planned
- 19: Successfully implemented
- 5: Not applicable

AMBER: partially implemented or planned

If you are relying on legitimate interests as the lawful basis for processing, your business has applied the three-part test and can demonstrate you have fully considered and protected individual's rights and interests.

Where measures have only been partially implemented, please select the appropriate actions from the detail below:

Suggested actions

You should:

- conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that you can justify your decision;
- if your LIA identifies significant risks, consider whether you need to do a data protection impact assessment (DPIA) to assess the risk and potential mitigation in more detail;
- keep your LIA under review, and repeat it if circumstances change; and
- include information about your legitimate interests in your privacy information.

Guidance

Guide to the GDPR – Legitimate interests, ICO website

Your business has established a process to recognise and respond to individuals' requests to access their personal data.

Where you have only partially implemented measures, please select the appropriate actions from the detail below:

Suggested actions

You should:

- ensure a process is in place to allow you to recognise and respond to any requests for personal data within the timescales;
- establish a policy on how to record any requests you receive verbally;
- include right of access procedures within your data protection policy;
- provide awareness training to all staff and specialist training to individuals who deal with any requests; and
- consider if you can provide remote access to a secure self-service system to provide the information directly to an individual in response to a request (this will not be appropriate for all organisations, but there are some sectors where this may work well).

Guidance

Guide to GDPR - Right of access, ICO website

Your business has identified whether any of your processing operations constitute automated decision making under Article 22 of the GDPR and has procedures in place to deal with the requirements.

Where you have only partially implemented measures, please select the appropriate actions from the detail below:

Suggested actions

You should:

- carry out a Data Protection Impact Assessment (DPIA) to identify whether any of your processing operations constitute solely automated decision making with significant effects ;
- establish whether you can rely on one of the GDPR exceptions for the processing and keep a record of it;
- identify the appropriate condition if you are processing special category personal data and keep a record of it;
- ensure you inform individuals about the processing in your privacy information;
- introduce a process for individuals to obtain an explanation of the decision and request a review; and
- implement procedures and safeguards to address the risks involved with this type of processing.

Guidance

Guide to GDPR - automated decision-making and profiling, ICO website

Guide to GDPR – Children, ICO website

Your business has a written contract with any processors you use.

Where you have only partially implemented measures, please select the appropriate actions from the detail below:

Suggested actions

You should:

- ensure that you have a written contract in place whenever you use a processor (a natural or legal person or organisation which processes personal data on your behalf);
- check both new and existing contracts in force oinclude certain specific terms, as a minimum, to ensure that data processing meets the requirements of the GDPR;.
- outline in the contract the technical and organisational arrangements the processor must have in place;
- include arrangements for security of processing, keeping records of processing activities, and notification of data breaches;
- refer to the ICO guidance (link below) to clarify responsibilities and liabilities, and to help you draft new contracts and amend existing ones. Please note that this guidance may be subject to change as our formal GDPR guidance evolves, so look out for publication of new ICO guidance.

Guidance

Guide to the GDPR – Contracts, ICO website

Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.

Where you have only partially implemented measures, please select the appropriate actions from the detail below:

Suggested actions

You should:

- have a clearly communicated set of security policies and procedures, which reflect business objectives and assign responsibilities to support good information risk management;
- ensure that you have processes in place to analyse and log any identified threats, vulnerabilities, and potential impacts which are associated with your business activities and information (risk register); and
- apply controls to mitigate the risks you've identified within agreed appetites and regularly test these controls to ensure they remain effective.

Guidance

The National Archives have produced some guidance on information risk management:

http://www.nationalarchives.gov.uk/information-management/manage-information/managing-risk/assessing-managing-risk/

Your business has a DPIA framework which links to your existing risk management and project management processes.

Where you have only partially implemented measures, please select the appropriate actions from the detail below:

Suggested actions

You should:

- review your existing risk and project management processes and ensure there is consistency and links with your DPIA processes in place;
- drive awareness of DPIAs across your business, and particularly amongst risk and project teams so that they understand the requirements; and
- ensure DPIA documentation is readily available for staff to use and that you have trained them on how to conduct the assessment.

Guidance

Guide to GDPR - Data protection impact assessment, ICO website

Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.

Where you have only partially implemented measures, please select the appropriate actions from the detail below:

Suggested actions

You should:

- ensure that any data you transfer outside the EU complies with the conditions for transfer set out in Chapter V of the GDPR;
- ensure that you have adequate safeguards and data security in place, that is documented in a written contract using standard data protection contract clauses; and
- implement measures to audit any documented security arrangements on a periodic basis.

Guidance

Guide to GDPR - International transfers, ICO website

GREEN: successfully implemented

Your business has conducted an information audit to map data flows.

Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Your business has identified your lawful bases for processing and documented them.

Your business has reviewed how you ask for and record consent.

Your business has systems to record and manage ongoing consent.

Your business has paid the data protection fee to the Information Commissioner's Office.

Your business has made privacy information readily available to individuals.

Your business has processes in place to ensure that the personal data you hold remains accurate and up to date.

Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked for it to be erased.

Your business has procedures to respond to an individual's request to restrict the processing of their personal data.

Your business has procedures to handle an individual's objection to the processing of their personal data.

Your business has an appropriate data protection policy.

Your business monitors its own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

Your business provides data protection awareness training for all staff.

Your business has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.

Your business understands when you must conduct a DPIA and has processes in place to action this.

Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

Your business has an information security policy supported by appropriate security measures.

Your business has effective processes to identify, report, manage and resolve any personal data breaches.

Not applicable

If your business relies on consent to offer online services directly to children, you have systems in place to manage it.

Your business communicates privacy information in a way that a child will understand.

If you may be required to process data to protect the vital interests of an individual, your business has clearly documented the circumstances where it will be relevant. Your business documents your justification for relying on this basis and informs individuals where necessary.

Your business has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.

Where required, your business has appointed a DPO. In other cases, you have nominated a data protection lead.

Thank you for completing this checklist. Please complete our short feedback survey to help improve our toolkit.

The survey should take around three minutes to complete.

Back