17 January 2019

Overall rating

Your overall rating was green.

- 0: Not yet implemented or planned
- 4: Partially implemented or planned
- 23: Successfully implemented
- 4: Not applicable

AMBER: partially implemented or planned

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.

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

Suggested actions

You should:

- ensure guidance is available for staff on the circumstances where they need to use this lawful basis for processing;
- review your existing processing to identify if you have any ongoing processing for this reason, or are likely to need to process for this reason in future; and then
- document where you rely on this basis and inform individuals if relevant.

Guidance

Guide to the GDPR – Vital interests, ICO website

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

Suggested actions

You should:

- implement a process that will enable individuals to submit a request to you;
- establish a policy on how you record any requests you receive verbally;
- have a process to allow you to recognise and respond to any individual requests in line with your legal obligations and statutory timescales;
- provide the personal data in a structured, commonly used and machine readable format;
- ensure that the medium in which you provide the data has appropriate technical measures in place to protect the data it contains; and
- ensure that the medium in which you provide the data allows individuals to move, copy or transfer that data easily from one organisation to another without hindrance.

Guidance

Guide to GDPR - right to data portability, ICO website

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

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

Suggested actions

You should:

- establish a process to monitor compliance to the policies;
- regularly test the measures that are detailed within the policies to provide assurances that they continue to be effective;
- ensure that responsibility for monitoring compliance with the policies is independent of the persons implementing the policy, to allow the monitoring to be unbiased; and
- report any results to senior management.

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

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.

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.

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

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 provides data protection awareness training for all staff.

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

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.

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

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.

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 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