21 March 2018

Overall rating

Your overall rating was amber.

- 7: Not yet implemented or planned
- 14: Partially implemented or planned
- 8: Successfully implemented
- 0: Not applicable

RED: not implemented or planned

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

Suggested actions

You should:

- Check that consent is the most appropriate lawful bases for processing.
- Make the request for consent prominent and separate from your terms and conditions.
- Ask individuals to positively opt in.
- Use unticked opt-in boxes or similar active opt-in methods.
- Use clear, plain language that is easy to understand.
- Specify why you want the data and what you're going to do with it.
- Give granular options to allow individuals to consent separately to different types of processing wherever appropriate.
- Name your business and any specific third party organisations who will rely on this consent.
- Tell individuals they can withdraw consent at any time and how to do this.
- Ensure that individuals can refuse to consent without detriment.
- Don't make consent a precondition of service.

Guidance

Guide to the GDPR - Consent, 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.

Suggested actions

You should:

- implement a process that will enable individuals to submit a request to you;
- 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 the data is provided has appropriate technical measures in place to protect the data it contains; and
- ensure that the medium in which the data is provided allows individuals to move, copy or transfer that data easily from one organisation to another without hindrance.

Guidance

Guide to the GDPR - Right to data portability, ICO website

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

Suggested actions

You should:

- review your processes and privacy notice(s) to ensure they inform individuals of their right to object "at the point of first communication". This information should be displayed or given clearly and separately from any other information;
- implement a process that will enable individuals to submit an objection request (this could include an online option);
- have processes in place to investigate an individual's objection to the processing of their personal data within the legitimate grounds outlined within the GDPR; and
- provide training or raise awareness amongst your staff to ensure they are able to recognise and respond (or know where to refer the request to) to an objection raised by an individual.

Your business has identified whether any of its processing operations constitute automated decision making and have procedures in place to deal with the requirements.

Suggested actions

You should:

- identify whether any of your processing operations constitute automated decision making;
- ensure that within any automated processing or decision making you undertake individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it;
- implement appropriate safeguards when processing personal data for profiling purposes; and
- ensure that any automated decisions do not contravene the restrictions outlined within Article9(2) of the GDPR.

Guidance

Guide to the GDPR - Rights related to automated decision making including profiling, ICO website

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

Suggested actions

You should;

- ensure that whenever your business uses a processor (a third party who processes personal data on your behalf) there is a written contract in place;
- check both new and existing contracts now include certain specific terms, as a minimum, to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
- determine whether it would be applicable to use standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) once drafted;
- investigate whether there are any approved codes of conduct or certification schemes that may be used to help you demonstrate that you have chosen a suitable processor; and
- use the ICO checklist (link below) to help you draft new contracts.

Guidance

Draft GDPR contracts guidance, ICO website

Guide to the GDPR - Contracts, ICO website

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

Suggested actions

You should:

- establish a policy which sets out when you should conduct a DPIA, who will authorise it and how it will be incorporated into the overall project plan. A DPIA screening process may be a useful tool in determining whether a DPIA is required;
- assign responsibility for completing DPIAs to a member of staff who has sufficient control over the project to effect change eg Project Lead/Manager;
- where a DPIA is required, ensure the process is completed before the project begins;
- ensure your process for completing a DPIA includes consultation with the DPO/ data protection lead, data processors, third party contractors and with the public/their representatives in most cases;
- ensure the information contained within the DPIA complies with the requirements under the GDPR and that the results are detailed within a report;

- where a DPIA indicates that the processing would result in a high risk and you are unable to mitigate those risks by reasonable means, ensure your business is aware to follow the ICO consultation process to seek its opinion as to whether the processing operation complies with the GDPR.

Guidance

Guide to the GDPR - Data protection impact assessments, ICO website

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

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 staff have had training on how to conduct the assessment.

AMBER: partially implemented or planned

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

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

Suggested actions

You should:

- organise an information audit across your business or within particular business areas to identify the data that you process and how it flows into, through and out of your business;
- ensure this is conducted by someone with in-depth knowledge of your working practices; and
- identify and document any risks you have found, for example in a risk register.

Guidance

Find out what information you have, National Archives

Identify information assets, National Archives

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

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

Suggested actions

You should:

- maintain records of processing activities detailing what personal data you hold, where it came from, who you share it with and what you do with it. This will vary depending on the size of your business;
- consider using an information asset register to do this; and
- ensure you have procedures to guide staff on how to manage information you hold.

Guidance

Identify information assets, National Archive

Information Asset Register template, National Archive

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

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

Suggested actions

You should;

- look at the various types of data processing you carry out;
- identify your lawful bases for carrying it out; and
- document it, for example in your privacy notice(s).

Guidance

Guide to the GDPR - Lawful basis for processing, ICO website

Your business has processes in place to ensure that the personal data it holds remains accurate and up to date

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

Suggested actions

You should:

- implement procedures to allow individuals to challenge the accuracy of the information you hold about them and have it corrected if necessary;
- have procedures to inform any data processors (third parties) you have disclosed the information about the rectification where possible;
- create records management policies, with rules for creating and keeping records (including emails);
- conduct regular data quality reviews of systems and manual records you hold to ensure the information continues to be adequate for the purposes of processing (for which it was collected);
- regularly review information to identify when you need to correct inaccurate records, remove irrelevant ones and update out-of-date ones; and
- promote and feedback any data quality trends to staff through ongoing awareness campaigns and internal training.

Guidance

Guide to the GDPR - Right to rectification, ICO website

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.

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

Suggested actions

You should:

- have procedures in place which allow individuals to request the deletion or erasure of their information your business holds about them where there is no compelling reason for its continued processing;
- have procedures to inform any data processors (third parties) you have shared the information with about the request for erasure;
- have procedures to delete information from any back up systems;

- implement a written retention policy or schedule to remind you when to dispose of various categories of data, and help you plan for its secure disposal;
- regularly review the retention schedule to make sure it continues to meet business and statutory requirements;
- assign responsibility for retention and disposal to an appropriate person;
- have appropriate methods of destruction in place to prevent disclosure of personal data prior to, during and after disposal; and
- if you use third parties to dispose of personal data ensure the contract includes the requirement for them to have appropriate security measures and the facility to allow you to undertake an audit.

Guidance

Disposal of Records, National Archives

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

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

Suggested actions

You should:

- review your procedures to determine where you may be required to restrict the processing of personal data;
- implement a process that will enable individuals to submit a request to you;
- have a process to act on an individual's request to block or restrict the processing of their personal data;
- have procedures to inform any data processors (third parties) you have shared the information with, if possible; and
- inform individuals when you decide to lift a restriction on processing.

Guidance

Guide to the GDPR - Right to restrict processing, 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 provides data protection awareness training for all staff.

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

Suggested actions

You should:

- provide induction training on or shortly after appointment;
- update all staff at regular intervals or when required (for example, intranet articles, circulars, team briefings and posters); and
- provide specialist training for staff with specific duties, such as marketing, information security and database management.

Guidance

Think privacy toolkit, ICO website

Training checklist for small to medium sized organisations, 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:

- establish a clearly communicated set of security policies and procedures, which reflect business objectives and assign responsibilities to support good information risk management;
- ensure there are 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 identified risks within agreed appetites and regularly test these controls to ensure they remain effective.

Guidance

Assessing managing risk, National Archives

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

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

Suggested actions

You should:

- look to continually minimise the amount and type of data you collect, process and store, such as by undertaking regular information and internal process audits across appropriate areas of the business;
- pseudonymise the personal data where appropriate to render the data record less identifying and therefore reduce concerns with data sharing and data retention;
- regularly undertake reviews of your public-facing documents, policies and privacy notice(s) to ensure they meet the renewed transparency requirements under the GDPR;
- ensure any current and/or new processes or systems enable you to comply with an individual's rights under the GDPR; and
- create, review and improve your data security features and controls on an ongoing basis.

Guidance

Guide to the GDPR - Data protection by design and default, ICO website

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.

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

Suggested actions

You should:

- clearly set out your business's approach to data protection and assign management responsibilities;
- ensure you have a policy framework and information governance strategy in place to support a positive data protection and security culture which has been endorsed by management;
- assess and identify areas that could cause data protection or security compliance problems and record these on your business's risk register;
- deliver training which encourages personal responsibility and good security behaviours; and
- run regular general awareness campaigns across your business to educate staff on their data protection and security responsibilities and promote data protection and security awareness and compliance.

Guidance

Think Privacy training, ICO website

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

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

Suggested actions

You should:

- develop, implement and communicate an information security policy;
- ensure the policy covers key information security topics such as network security, physical security, access controls, secure configuration, patch management, email and internet use, data storage and maintenance and security breach / incident management;
- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with your security policy

- implement periodic checks for compliance with policy, to give assurances that security controls are operational and effective; and
- deliver regular staff training on all areas within the information security policy.

Guidance

The ICO has previously produced guidance to assist organisations in securing the personal data they hold. We are working to update existing guidance to reflect GDPR provisions and once completed, this section will expand to include this information.

In the meantime, the existing guidance is a good starting point for organisations. This is located in the guidance index under the 'security' heading.

Small businesses guidance, National Cyber Security Centre 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 is handled in compliance with the conditions for transfer set out in Chapter V of the GDPR;
- ensure that there is 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 the GDPR - International transfers, ICO website

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

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

Suggested actions

You should:

- train staff how to recognise and report breaches;
- have a process to report breaches to the appropriate individuals as soon as staff become aware of them, and to investigate and implement recovery plans;
- put mechanisms in place to assess the likely risk to individuals and then, if necessary, notify individuals affected and report the breach to the ICO; and
- monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

Guidance

Guide to the GDPR - Data breaches, ICO website

GREEN: successfully implemented

Your business has systems to record and manage ongoing consent.

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

Your business is currently registered with the Information Commissioner's Office.

Your business has made privacy notices readily available to individuals.

If your business offers online services directly to children, you communicate privacy information in a way that a child will understand.

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

Your business has an appropriate data protection policy.

Your business has nominated a data protection lead or Data Protection Officer (DPO).

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