Chartered Institute of Internal Auditors

21 September 2020

GDPR as BAU: are your processes in place?

Chartered Institute of Internal Auditors

As you will be aware the General Data Protection Regulation (GDPR) came into force 25 May 2018 – a full two years after the European Parliament passed legislation. This legislation significantly extended protection of private data, with increased responsibilities and consequences for organisations. As GDPR applies to all EU citizens, an organisation holding or processing even one EU citizen's data must comply. The fines are significant compared to previous penalties: 4% of annual turnover or €20 million, whichever is greater.

The two years between GDPR becoming law and coming into force gave time to prepare. To this end, the Chartered IIA has been keen to provide information and support to its members, through technical guidance, blogs and events. Organisations are looking to internal audit to provide guidance and assurance on this most business-critical area.

So, what has happened since 25 May this year, and what will happen as we move into 2019? An Imperva study quoted by the Chartered IIA in Risk in Focus 2018 showed how much work remained to raise awareness. '51% of executives and IT security professionals believed GDPR would impact their companies, 33% didn't see it impacting them, 11% were unsure and 5% were not familiar with GDPR.' Following on from this a study by TrustArc quoted in Risk in Focus 2019 states that only 27% of businesses in the EU reported being compliant with GDPR one month after the enforcement date of 25 May 2018. However, 74% expect to be compliant by the end of 2018 and 93% by the end of 2019.

As late as the week before the deadline, many internal auditors were concerned that their organisations had still not fully grasped the scope of GDPR. Some saw it as purely an IT matter; others referred it to legal teams. However, to comply with the spirit and the letter of the law, awareness must come from the top down.

If certain organisations were still unaware of GDPR's meaning and importance, many members of the public were aware. Within 24 hours of GDPR coming into force, individuals brought claims against Facebook, Google's Android operating system, Instagram and WhatsApp. Data regulators in the UK, France, Austria and elsewhere in the EU reported a sharp rise in complaints. This suggests that the public as a whole is ready to hold organisations to account. Has your organisation received any complaints from your customers, what actions have been taken, would you as internal audit be aware if they had?

There were also consequences for organisations that, keen to demonstrate compliance, contacted all customers to seek explicit permission for continued communication. This was unnecessary in many instances and led to customers expressing anger and frustration at the emails clogging up their in-boxes.

As we highlighted earlier this year in our blog Keeping current with consent, consent forms and

emails are not the only tools available. Consent is only one of eight grounds for holding or processing data. The other seven are:

1. Contract
2. Legal obligation
3. Vital interests
4. Public task
5. Legitimate interests
6. Special category data
7. Criminal offence data

Some global organisations have been told by their legal teams that consent is the only avenue to compliance. Given this lack of awareness, internal auditors should be ready to support and guide with the correct advice. Seeking consent when it is not necessary could lead to significant reputational risk and – if customers leave out of irritation – financial loss. Keep in mind, too, that if your organisation has fewer than 250 employees, your regulatory obligations are fewer.

So what should internal audit be doing to help organisations nearly six months on?

Every affected organisation, whether private, public or third sector, should start with the first of the Information Commissioner's Office 12 Steps: awareness. Even the best-organised company, government department or charity, fully compliant from before 25 May, must remain aware to remain compliant. Knowing what information, you hold, why, how and where is essential.

Internal audit can and should already be involved in data protection impact assessments (DPIAs). These exercises, mandated by GDPR, should make clear on which lawful basis the organisation is holding or processing data. If your organisation is not yet fully compliant, or not able to demonstrate and document compliance, the assessments can at least show that you are acting in good faith to fill gaps and improve.

Risk in Focus 2019

Here are the key questions that have been highlighted on data protection:

- Is the organisation compliant with GDPR and, if necessary, China's Personal Information Security Specification?
- Are US companies that share the organisation's personal data certified under the EU-US Privacy Shield scheme?
- How is personal and operationally/strategically sensitive data shared with third parties and how do you know these parties are keeping it secure?
- Are senior management and the compliance function aware of the need to remain compliant as the company and the ways in which it collects and uses personal data evolves?
- Is the compliance function in close communication with the data management function so that the former is aware of how any company changes may impact upon GDPR compliance?
- Is there a data strategy for how the organisation uses data, personal or otherwise, to its advantage? Is this aligned with the corporate strategy?
- How does the strategy envisage data being used in the future? Is this clear and well-articulated?
- Is the internal audit function prepared to advise the Chief Data Officer and/or data management function with any changes to the organisation's use of data by providing a risk control

perspective?

Download Risk in Focus

Internal audit assurance

These are just some of the other ways internal audit can provide assurance.

- Review previous data-related audit findings and conclusions in high-risk areas. Keep an open mind for themes – improving data protection in one area may improve it in several.
- Don't forget the paperwork – there may be areas that are very low-tech but still data-heavy. Have these areas been overlooked? It can easily happen if their data isn't centrally captured or mined.
- Communicate – however busy you are, make sure that regular meetings with the audit committee, board and senior management include GDPR.
- Keep in touch throughout the business to detect any unaddressed or newly emerging risks and assess management response.
- And, of course, amend the audit plan to include necessary consultancy and assurance engagements. Risk-based internal audit exists only when you are alert and responsive to changes both inside and outside our organisations.

12 steps to data compliance

The Information Commissioner's Office has updated its 12 steps to data compliance:

1. Awareness
Check if you are a Competent Authority under Schedule 7 of the DP Act 2018 or have statutory functions for any of the law enforcement purposes. If so, you should make sure that key people in your organisation are aware that as of May 2018, the law has changed.

2. Information you hold - mapping
You should document what personal data you hold, where you hold it, where it came from, who you share it with and who is responsible for it. Identify what personal data is being processed under Part 3 (of the DP Act 2018) and what is being processed under other parts of the Act and GDPR. Do you work jointly with other organisations? Do you use data processors? You may need to organise an information audit and review any contracts or agreements.

3. Lawful basis for processing data
You should identify the lawful basis for your processing activity, document it and update your privacy notices to explain it, using clear and plain language.

4. Consent
If you rely on consent you need to consider whether this is appropriate or whether you should use another lawful basis. If consent is appropriate then you should review how you seek, record and manage consent and whether you need to make any changes. You will need to refresh existing consents if they do not meet the standard required.

5. Privacy notices
You should review your current privacy notices and ensure that these are in an easily accessible

form and up-to-date. You will need to include more detailed information including your lawful basis for processing personal data and retention periods unless an exemption applies.

6. Individuals' rights

You should check your procedures to ensure they cover all the rights individuals may have, including deletion, so that you know how to respond within the specified timescales

7. Data breaches

You should ensure that you have the right procedures in place to identify, manage and investigate a breach. You will need to have processes in place to determine whether you need to report the breach to the ICO, based on the risks to individuals' rights and freedoms. If you decide that it is necessary to report you will need to do so no later than 72 hours after becoming aware of it. You should be prepared to notify affected individuals in some cases.

8. Data protection by design and data protection impact assessments

Make sure you are familiar with the ICO's code of practice on privacy impact assessments as Data Protection Impact Assessments are now mandatory where any processing is likely to result in a high risk to the rights and freedoms of individuals.

9. Data Protection Officers

Ensure you designate someone to take responsibility for your data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You are now required to have a Data Protection Officer (unless you already have one under the requirements of the GDPR or a specific piece of European law enforcement legislation),

10. Logging

You should ensure that you are able to keep logs of processing operations in automated processing systems. This will include a log of any alterations to records, access to records, erasure and disclosures of records unless an exemption applies.

11. International

You should review procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure that they are compliant.

12. Sensitive processing

If you are undertaking sensitive processing you will need to ensure that you are compliant with the requirements of the legislation including having an appropriate policy in place.

Finally, the ICO's Guide to the GDPR is a 'living document', so do bookmark it and check back regularly to keep abreast of updates.

Further reading

Risk in Focus 2019
Risk in Focus 2018

Guidance

Data protection

External resources

Information Commissioner's Office:

12 steps to data compliance
Guide to the General Data Protection Regulation