Chartered Institute of Internal Auditors

21 September 2020

GDPR: What? When? Why?

Chartered Institute of Internal Auditors

The General Data Protection Regulation (GDPR) has been on many organisations' corporate minds, and rightly so, for some time. However, with the regulation coming into force on 25 May 2018, awareness must now become action – and internal audit should be involved at all levels, to help management better understand and mitigate the related risks.

What? When? Why?

The European Parliament passed GDPR on 27 April 2016 through European Directive 2016/679 'on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)'. The previous regulation had led to data protection legislation in all member states, such as the UK's Data Protection Act of 1998. While this approach allowed for national legislation to reflect national concerns and priorities, it led to a 'patchwork of rules', as the ACCA has phrased it: Any company handling the data of EU residents should start preparing now for its stringent new data-protection rules.

GDPR brings in a single piece of legislation across member states, while still allowing for 'derogation', whereby member states may adapt the legislation in certain situations. The UK was a strong supporter of the move to reform data protection, not only to bring about greater harmonisation, but also to take into account the massive social and technological changes of the past 20 years.

More data, and more personal data, is being shared than ever before, and both cyber-commerce and the digital economy as a whole are increasing daily. As more people trust their information to virtual rather than physical businesses and platforms, it seems appropriate that the laws governing that information and its safe use keep pace.

Significant differences between the DPA and GDPR include the introduction of:

1. explicit guidance on how children's data and data consent should be managed
2. the highly publicised 'right to be forgotten', also known as the right of erasure
3. data portability – individuals will have the right to request their data in an easily accessible, portable yet secure format
4. the need to appoint data protection officers and, in many organisations, a representative based in an EU member state
5. increased accountability and consequences for individuals and organisations who hold and/or

process personal data
6. reduced timescales to report data breaches and respond to subject access requests
7. greater consequences for non-compliance.

Whatever your organisation's purpose, sector or location, you are overwhelmingly likely to need to comply with, and demonstrate compliance with, GDPR. Customers, members of staff, members of the public who share personal data of any sort – any individual who interacts with your organisation is protected.

Only until Brexit, you may be thinking – but you'd be wrong. The UK Government announced, in a statement of intent on 7 August 2017, its commitment to bring GDPR into local legislation. This means that there should be legislative equivalence between GDPR and whatever UK law seeks to mirror or duplicate it.

The need for the UK Government to do so is obvious: failure to comply with GDPR, or demonstrate an equal standard in home legislation, would leave any UK organisation holding personal data on any EU citizen exposed to the consequences of non-compliance.

Not only would this mean potential fines far exceeding any current penalty, but also the possibility of criminal charges. It will be a criminal offense to knowingly be reckless with personal data, or to allow circumstances in which 'anonymised' data could nonetheless identify people.

In the Republic of Ireland, GDPR will have direct effect and so not require additional national legislation. The Irish Data Protection Commissioner has been working throughout 2017 to raise awareness within government and throughout organisations of the need for increased transparency, security and accountability.

Organisations cannot approach GDPR as a purely legal or IT matter – it will have to be led, implemented and reinforced across the organisation, with continuous and collaborative involvement from legal, IT, compliance, risk and internal audit teams.

As you can imagine, this will require even those organisations currently fully compliant with the DPA to conduct extensive gap analyses and data audits in order to develop GDPR compliance plans.

As always, governance is and will be key. Relationships across the business, especially at board and audit committee level, will help internal audit gain sight of and provide assurance about levels of understanding and readiness. Internal audit's expertise and insight should equip it to play a significant role at every stage of preparation for and compliance with GDPR.

So what?

If your organisation has been complacent or dilatory about data protection, information or cyber security, or compliance with the DPA, GDPR should concentrate minds urgently.

Non-compliance is not an option, unless anyone fancies eye-watering fines of up to €20 million or 4% of annual turnover – whichever is greater. Most organisations will take fright – and rightly so – at the scale of financial risk implied by the increased fines. They're certainly higher than the current £500,000 limit the Information Commissioner's Office (ICO) can levy in theory. But fines and associated negative publicity are not the only risk.

Financial, including regulatory

Financial costs of non-compliance are, as stated above, significant, on a scale that could bankrupt smaller or more financially compromised organisations. The stakes are higher for both organisations and employees, as both data controllers and data processors are responsible and therefore liable.

Several analyses to date have focussed on the financial services sector as one that will require, and possibly receive from the regulator, particular attention. Certainly the potential for both breaches and headline-grabbing fines is there, but most banks have the financial resources to pay fines.

Can we say the same for the public sector, or third-sector bodies such as charities? And yet these are the organisations holding personal data on some of the most vulnerable people in society.

Other financial risks of non-compliance are legal costs and possibly damages paid to litigants, if people decide to sue an organisation for mishandling their personal data. There are also significant costs associated with preparing for GDPR.

Poor or no planning – 'We'll cross that bridge when we come to it' – has its own risks. Although the UK regulator has hinted it will accept firms 're-papering' contracts on a rolling basis', as the contracts come up for renewal, it is still a tricky option, leaving the possibility of litigation and reputational risk still open. It would also leave UK business liable to censure from non-UK regulators, where business operates outside the UK but elsewhere in the EU.

Some managers may balk at the costs of being fully compliant by May 2018, citing budget constraints, and feel that a phased approach is appropriate. But imagine the costs of 'just-in-time', last-minute or urgent remedial work on this scale.

New systems are costly, and highly sought-after consultants with IT, legal, compliance and safeguarding expertise will all be that much more expensive if contracted at short notice. And remember, even though you outsource an activity, you cannot outsource the risk!

Reputational

As GDPR has shown, the world is now one of immediate virtual connection. Proven non-compliance, especially if accompanied by a hefty fine, would be headline news nationally and possibly globally. And news, fake or otherwise, spreads instantaneously. The very platforms GDPR is designed to account for, especially social media, are those that guarantee notoriety in seconds for any real or perceived breach.

What's more, children and vulnerable adults are now freer to express themselves and interact online, while at the same time being subject to ostensibly greater concern and protection. The same parents who may allow their children unlimited screen time will be the first to name and shame, and report to the authorities, any service provider or other organisation they feel has failed in its duty of care to their offspring.

And what of schools, hospitals, GPs' surgeries, social services, police forces, probation offices and charities working with vulnerable people? Many of these organisations have few resources, yet greater responsibility and potential exposure to censure, than any private-sector company such as a global financial services firm. Public and third-sector 'client' data is potentially far more intimate or compromising than that held by the average bank.

So what action can organisations take to mitigate these risks? As you would expect, well-designed

responses should mitigate the most serious risks. The organisation should focus on a few key controls that will give the broadest and best comfort.

Likely responses

- Gap analysis; results needing action should appear on risk register.
- Data protection impact assessment (mandated by GDPR).
- Frequent, meaningful reporting of progress towards GDPR, reviewed by board and executive.
- Remedial work – as part of (business as usual) BAU or GDPR-specific projects.
- Organisation-wide communications and training (one of most important mitigants of consequences of a breach, and so should be high priority for all organisations).

Ways internal audit can provide assurance

- Thematic review of likely areas of highest risk based on previous audit findings.
- Q4 2017-Q1 2018: amend the audit plan to include necessary consultancy and assurance engagements.
- Monthly meetings with audit committee, board and senior management to raise awareness, increase executive support and track progress.
- Regular engagement throughout the business to detect any unaddressed or newly emerging risks and assess management response.

What next?

Internal audit can and should take the lead before, during and after 25 May 2018. If your function has not yet been involved, then make sure you are! It will mean adjusting your annual audit plan and beyond, but GDPR is exactly the kind of event that should, in risk-based auditing terms, be top priority. Providing consultancy and advisory services throughout the organisation, internal audit can firstly advise on and assess the governance over GDPR.

Consultancy engagements can assess organisational readiness for 25 May, whereas assurance engagements will assess whether the organisation is compliant as of 25 May. Whether at board level or below, how senior leaders and decision-makers approach GDPR and communicate its importance to their colleagues will influence how compliant and successful the organisation is.

Internal audit should be constantly creating and building relationships at all levels of the organisation. This does not mean telling people what they want to hear, but rather developing a mature, professional basis to exchange information and views. Only when internal audit makes its voice heard can it truly help enhance risk management and provide meaningful assurance.

GDPR will be either a test or confirmation of many internal audit functions' place and influence. According to the ICO, there are 12 steps all organisations need to take now to prepare for GDPR:

1. Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information you hold

You should document what personal data you hold, where it came from and who you share it with.

You may need to organise an information audit.

3. Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Lawful basis for processing data
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. Consent
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. Children
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data protection by design and data protection impact assessments
You should familiarise yourself now with the ICO's code of practice on privacy impact assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. Data protection officers
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a data protection officer.

12. International
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

How many of these will require or benefit from internal audit insight, either through consultancy or assurance engagements, before, during and after GDPR comes into force? You may want to use the table below to check that your internal audit function is involved in all relevant aspects of your organisation's GDPR activity.

Crucial activities for Q4 2017 and Q1 2018 will include checking GDPR information on your organisation's risk register. Is it complete and realistic? Does it show a true understanding of risks and controls as they apply to GDPR? Do the organisation's board, audit committee and executives ask for meaningful information as work progresses?

How about data protection and privacy impact assessments? These are required by the legislation and will be necessary well in advance of 25 May 2018.

Throughout preparation, internal audit needs to help raise awareness at all levels of the organisation and promoting a risk-based approach at all times.

After May 2018, internal audit, while still valued for its consultancy work and insights is likelier to emphasise assurance. How adequate and effective are the policies and processes in place as controls? What about the biggest control of all – governance? Are the right people in the right roles to promote sound data controlling and processing? How rigorous and timely is the reporting of data breaches? Are we fully compliant? How do we learn from incidents?

Once GDPR has started to become business as usual, how will internal audit reflect this in its annual plans? Should GDPR be a consideration for every audit engagement, in the way culture now should be?

Is auditing the GDPR control framework also something that should happen across the organisation every two to three years? Your response will depend on the size, nature and risk maturity of your organisation.

Specific areas will need greater focus before, during and after implementation. IT and GDPR-specific change programmes are obvious examples, but organisation-wide communications will need to ensure that GDPR stays topical even after the initial rush of activity.

Do your human resources or learning and development teams have plans to amend training for existing staff and new joiners? If not, they should; and if they do, you'll want to check that GDPR remains a significant topic for induction and refresher training.

There are currently gaps in the guidance available, but this will develop as everyone gets to grip with GDPR. Your role in internal audit should include staying abreast of any changes to legislation, guidance and good practice – whether in your industry or elsewhere. Excellent articles on, for instance, how GDPR is likely to affect financial services can still spark useful ideas in other sectors. Everyone everywhere will be affected.

Self-assessment table

Use this for internal audit involvement in GDPR activity before, during and after 25 May 2018 for both consultancy and assurance engagements.

ICO's 12 steps to take for GDPR	Pre May 2018	May 2018	Post 25 May 2018
Awareness			

Information you hold			
Communicating privacy information			
Individuals' rights			
Subject access requests			
Legal basis for processing personal data			
Consent			
Children			
Data breaches			
Data protection impact assessments			
Data protection officers			
International			

Further reading

Standards

Attribute

1220.A2: In exercising due professional care internal auditors must consider the use of technology based audit and other data analysis techniques.

Performance

2050 - Coordination and Reliance: The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimise duplication of efforts.

2120.A1 - Risk Management: The internal audit activity must evaluate risk exposures relating to the organisation's governance, operations, and information systems regarding the:

- Achievement of the organisation's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

2130.A1 - Control: The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organisation's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

Implementation guides

Due professional care
Coordination and reliance
Risk management
Control

Supplemental guidance

Auditing privacy risks (2nd ed.)
Auditing the control environment
Coordination of assurance services
Integrated Auditing
Internal audit and the second line of defense
Reliance by internal audit on other assurance providers
GTAG and GAIT resources

Guidance: Cyber security
Blog: GDPR: Mountain or molehill
Board briefing: Cyber security

External resources

Original text of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016
Overview of the GDPR from the UK Information Commissioner's Office (ICO)
Preparing from the GDPR: 12 steps to take now (UK ICO)
GDPR guidance from the Irish Data Protection Commissioner
Dedicated GDPR site from the Office of the Information Commissioner (Jersey) and the Office of the Data Protection Commissioner (Guernsey) including a valuable overview of GDPR from a Channel Islands perspective:
ACCA CPD article on GDPR
DLA Piper document on key changes arising from GDPR

Risk.net - Risk management article with financial services focus, but useful for all sectors - boiling the ocean gdpr data demands overwhelm banks