Incorporating GDPR Into IT Audits

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/36OGNru

It is now almost two years since the EU General Data Protection Regulation (GDPR) was enacted. Since then, a lot has been written about the regulation. Indeed, a quick Google search produces about 486,000,000 results.[1] Given the elapsed time since it came into effect, GDPR should now be business as usual. Certainly, IT auditors should be considering the regulation for all audits where personal data[2] are processed. So, what aspects of the regulation should be considered while auditing an application's general IT controls?

GDPR consists of 99 articles; however, many of these define the overall rules for the regulation. These have been well documented in two audit programs published by ISACA®.[3,4] Here, the focus is on GDPR articles that I believe are applicable across any IT application-focused audit where personal data are processed.

Article 30: Records of Processing Activities

Article 30 requires that each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.[5] The starting point of the audit should be to request a copy of these records, as they allow one to understand the purposes of the processing, provide a description of the categories of both data subjects and personal data, and ascertain whether any third parties or, indeed, third countries are involved. Where this is not in place and one understands that personal data are processed, this should be an audit finding. An article 30 example is provided in ISACA's GDPR Audit Program Bundle.[6]

Article 6: Lawfulness of Processing

For processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis.[7] From an audit perspective, one should confirm that this consent has been captured, as the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.[8] For a given application, this consent may be stored in the database for each data subject. If so, this should be reviewed. Other legal bases exist and a test in ISACA's GDPR Audit Bundle requires that these are documented in the Records of Processing Activities (Article 30).[9]

One such legal basis is legitimate interests, which refers to the interests of the enterprise under review or the interests of third parties. These can include commercial interests, individual interests or broader societal benefits.[10] Legitimate interests are different than other lawful bases, as they are not centered around a particular purpose and they are not processing to which the individual has specifically agreed (consent). Legitimate interests are more flexible and could, in principle, apply to any type of processing for any reasonable purpose.[11] For this reason, it is important to confirm that a legitimate interests assessment has been performed and that a record of it has been kept in order to justify the enterprise's decision.[12] Again, this could be stored with the Records of Processing Activities (Article 30).[13]

Ian Cooke, CISA, CRISC, CGEIT, COBIT 5 Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, FIP, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has over 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees, was a topic leader for the Audit and Assurance discussions in the ISACA Online Forums and is a member of ISACA's CGEIT® Exam Item Development Working Group. Cooke has supported the update of the CISA® Review Manual and was a subject matter expert for the development of ISACA's CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules and the 2020 Michael Cangemi Best Book/Author Award. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), LinkedIn (*www.linkedin.com/in/ian-cooke-80700510/*), or on the Audit and Assurance Online Forum (*engage.isaca.org/home*). Opinions expressed are his own and do not necessarily represent the views of An Post.

Article 9: Processing of Special Categories of Personal Data

Article 9 of GDPR states that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation shall be prohibited.[14] It includes a number of exceptions such as explicit consent.

From an audit perspective, it is vital to confirm that this explicit consent is captured, perhaps in the application's database at the data subject level and that, again, the purposes have been documented. Once again, an example is available in ISACA's GDPR Audit Bundle.[15] For both Articles 6 and 9, it is likely that a data classification exercise[16] was performed. This should be reviewed.

Article 15: Right of Access by the Data Subject

According to Article 15, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data.[17] In addition, much of the information captured under Article 30 should be made available to the data subject. Article 12 states the information shall be provided in writing or by other means, including, where appropriate, by electronic means.[18] This has been interpreted to mean that where the request is made by electronic means that the information should be provided in a commonly used electronic form. Indeed, where possible, the controller should be able to provide remote access to a secure system, which would provide the data subject with direct access to his or her personal data.[19]

Therefore, from an audit perspective, it is important to ensure that there is a defined mechanism to provide this access or to otherwise electronically output all the personal data that the application stores. This may take the form of simple print screens; nonetheless, a process should be defined and demonstrable.

Article 16: Right to Rectification

Article 16 of GDPR states that the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.[20] As most applications, by their very nature, allow for the rectification of data, this should be a relatively straightforward right with which to comply. Nonetheless, the IT auditor should ensure that a process exists that allows for the rectification of the data in the application under review.

Article 17: Right to Erasure ("Right to Be Forgotten")

According to Article 17, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.[21] However, this is not an absolute right, and the article details specific rules about when this applies, including exemptions.

If a valid erasure request is received, then one will have to take steps to ensure erasure from backup systems as well as live systems. One must be clear with the individual as to what will happen to their data when their erasure request is fulfilled, including with respect to backup systems. It may be that the erasure request can be instantly fulfilled with respect to live systems, but that the data will remain within the backup environment for a certain period until it is overwritten.[22]

Enjoying this article?

- Read *How to Audit GDPR. www.isaca.org/how-to-audit-GDPR*
- Learn more about, discuss and collaborate on audit and assurance ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Auditors should confirm that a mechanism exists to delete the data and that the process around backups is known and documented so that the data subject can be informed.

Article 18: Right to Restriction of Processing

Article 18 of GDPR states that the data subject shall have the right to obtain from the controller restriction of processing in certain circumstances.[23] Again, this is not an absolute right. The important thing to consider from an IT audit perspective is how would the processing be restricted in the application under review? Is there a mechanism to allow this?

Article 20: Right to Data Portability

Article 20 of GDPR says that the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.[24] In addition, where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.[25]

From an IT audit perspective, it is important to ensure that any personal data can or could be exported from the application. Where industry groups are in place (e.g., banking), it may be important to demonstrate a readiness to develop an interoperable format.[26]

Article 25: Data Protection by Design and by Default

According to Article 25, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the regulation and protect the rights of data subjects.[27]

Auditors should confirm that Privacy by Design principles[28] were considered and documented for any significant changes or developments for the application under review.

The term "pseudonymization" needs more clarity. Pseudonymization of data means replacing any identifying characteristics of data with a pseudonym or, in other words, a value that does not allow the data subject to be directly identified.[29] GDPR defines pseudonymization as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that a) such additional information is kept separately, and b) it is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

> "FROM AN IT AUDIT PERSPECTIVE, IT IS IMPORTANT TO ENSURE THAT ANY PERSONAL DATA CAN OR COULD BE EXPORTED FROM THE APPLICATION."

Article 32: Security of Processing

Article 32 requires that the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including *inter alia,* as appropriate:[30]

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

This is more familiar ground for IT auditors, and the controls documented in, for example, the International Organization for Standardization (ISO) standard ISO 27001 *Information Security Management System* and/or the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* can be used to demonstrate compliance. Good guidance is also provided in the GDPR Audit Bundle.[31]

Article 35: Data Protection Impact Assessment

Article 35 of GDPR requires that where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[32]

Fundamentally, this is a risk assessment, but it should be conducted from the perspective of the data subjects. GDPR does not define "likely to result in high risk." However, the important point here is not whether the processing is actually high risk or likely to result in harm—that is the job of the Data Protection Impact Assessment (DPIA) to evaluate in detail. Instead, the question is a more high-level screening test or a threshold analysis: Are there features that point to the potential for high risk?[33]

From an IT audit perspective, where significant changes have been made to the application under review, it is important to confirm that a threshold analysis and/or a DPIA has been performed and has been documented.

"FROM AN IT AUDIT PERSPECTIVE, WHERE SIGNIFICANT CHANGES HAVE BEEN MADE TO THE APPLICATION UNDER REVIEW, IT IS IMPORTANT TO CONFIRM THAT A THRESHOLD ANALYSIS AND/OR A DPIA HAS BEEN PERFORMED AND HAS BEEN DOCUMENTED."

Conclusion

Despite some commentary to the contrary, GDPR was not and is not a Y2K-type project. Besides the need for ongoing GDPR conformance,[34] at a business and operational level, the regulation has resulted in several requirements that should be considered when auditing any application where personal data[35] are processed. These requirements should now be business as usual for all IT auditors conducting such reviews.

Endnotes

1 Accessed 9 October 2019
2 This also depends on the territorial scope. See European Data Protection Board, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), Version 2.0, 12 November 2019, *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf*
3 ISACA®, GDPR Audit Program Bundle, USA, 2018, *https://next.isaca.org/bookstore/COBIT-5/WAGDPR*
4 ISACA, GDPR Audit Program for Small and Medium Enterprises, USA, 2019, *https://next.isaca.org/bookstore/COBIT-5/WAUGDPR*
5 Intersoft Consulting, Art. 30 GDPR, Right of Access by the Data Subject, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-30-gdpr/*
6 *Op cit*, GDPR Audit Program Bundle
7 Intersoft Consulting, Recital 40 Lawfulness of Data Processing, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/recitals/no-40/*

8 Intersoft Consulting, Art. 7 GDPR, Conditions for Consent, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-7-gdpr/*
9 *Op cit* Art. 30 GDPR
10 Information Commissioner's Office, Legitimate Interests, United Kingdom, *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/*
11 Information Commissioner's Office, What Is the "Legitimate Interests" Basis? United Kingdom, *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/*
12 *Op cit* Legitimate Interests
13 *Op cit* Art. 30 GDPR
14 Intersoft Consulting, Art. 9 GDPR, Processing of Special Categories of Personal Data, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-9-gdpr/*
15 *Op cit* GDPR Audit Program Bundle
16 Cooke, I.; "Doing More With Less," *ISACA® Journal*, vol. 5, 2017, *https://www.isaca.org/archives*
17 Intersoft Consulting, Art. 15 GDPR, Right of Access by the Data Subject, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-15-gdpr/*
18 Intersoft Consulting, Art. 12 GDPR, Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-12-gdpr/*
19 Intersoft Consulting, Recital 63, Right of Access, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/recitals/no-63*
20 Intersoft Consulting, Art. 16 GDPR, Right to Rectification, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-16-gdpr/*
21 Intersoft Consulting, Art. 17 GDPR, Right to Erasure ("Right to be Forgotten"), EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-17-gdpr/*
22 Information Commissioner's Office, Right to Erasure, United Kingdom, *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/*
23 Intersoft Consulting, Art. 18 GDPR, Right to Restriction of Processing, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-18-gdpr*
24 Intersoft Consulting, Art. 20 GDPR, Article 20, Right to Data Portability, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-20-gdpr/*
25 Intersoft Consulting, Recital 68, Right of Data Portability, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/recitals/no-68/*
26 *Ibid*.
27 Intersoft Consulting, Art. 25 GDPR, Data Protection by Design and by Default, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-25-gdpr/*
28 Agencia Española de Protección de Datos, A Guide to Privacy by Design, Spain, 2019, *https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf*
29 Data Protection Commission, *Guidance Note: Guidance on Anonymisation and Pseudonymisation*, Ireland, June 2019, *https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf*
30 Intersoft Consulting, Art. 32 GDPR, Security of Processing, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-32-gdpr/*
31 *Op cit* GDPR Audit Program Bundle
32 Intersoft Consulting, Art. 35 GDPR, Data Protection Impact Assessment, EU General Data Protection Regulation, Belgium, 2017, *https://gdpr-info.eu/art-35-gdpr/*
33 Information Commissioner's Office, When Do We Need to Do a DPIA?, United Kingdom, *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/*
34 Cooke, I.; "Assurance Considerations for Ongoing GDPR Conformance," *ISACA® Journal*, vol. 1, 2019, *https://www.isaca.org/ archives*
35 *Op cit* Guidelines 3/2018 on the Territorial Scope of the GDPR