DBS Business Review 01| 2017
PRACTITIONER UPDATE | dbsbusinessreview.ie

Data Protection in EU Businesses: an Introduction to GDPR

Jack Hyland
IReL Manager
University College Dublin
Dublin, Ireland

Irish businesses can't have failed to notice the increasing number of news items on data breaches in organisations. These have included major stories about malicious attacks on multinationals (affecting Sony and Yahoo recently) but also national reports about flaws in data management practices: for example, the Irish civil servants' payroll system has been plagued by a series of data breaches in recent years (Edwards, 2017). Indeed the ongoing Maurice McCabe scandal is, in part, a story of a multi-organisation and multi-level failure to adhere to basic principles of an individual's data privacy rights.

All organisations, big and small, are responsible for managing private data of varying volumes, from the massive amount of personal information passing through social media multinationals, to SMEs managing employees' payroll and customers' contact details. So it is timely to raise awareness of the European Union's General Data Protection Regulation (GDPR), which will become law across the EU from May 2018. The GDPR will affect how Irish and European businesses collect, retain and share personal data and significant fines will be applicable to organisations in breach of it. The Data Protection Commissioner (DPR) will also have the power to stop organisations collecting data and force them to delete it.

The GDPR is designed to harmonise and strengthen European citizens' data privacy and to provide a consistent playing field for companies doing business across the EU. It covers any data that could be used to identify a person: their name, date of birth, or their IP address, but also information about personal characteristics such as their age, gender or nationality.

GDPR means businesses must explicitly seek consent from their customers when collecting information. Customers have the right to know what details are stored about them and they have the right withdraw consent about allowing businesses to keep this information. All organisations must have procedures in place to notify individuals when potentially harmful data is breached and they may need to report it to the Data Protection Commissioner.

International Data Transfers and Privacy Shield

The GDPR prohibits companies from transferring personal data outside of the European Economic Area but the EU-US Privacy Shield agreement (EU-US Privacy Shield 2017) allows European companies to continue to keep the data in the cloud using US-based companies (Google, Dropbox, Amazon etc.). However, Privacy Shield may be challenged in court so businesses should explore a longer term Plan B: making sure their data in the cloud stays within the EEA (Lonergan, 2017).

Subject access requests

The GDPR means that customers have the right to access their personal information, to have their data corrected or erased. Research from 2015 suggests a large percentage of Irish companies will not be compliant: only 40% of companies in the study were able to comply with current legislation for subject access requests (Castlebridge Associates, 2017). So organisations need to consider the following:

- How can individuals make requests (online, by phone, in person, etc.)
- The length of time to process requests
- The volume of requests anticipated and the logistics of managing this.

Gathering data

Before gathering any personal data, companies must notify customers in clear language about the company's identity, why they need the data and how they will use it (sharing with third parties etc.). What customers are consenting to should be clearly explained and companies must maintain a record proving that consent was given.

Retaining data

Organisations will not have the right to retain personal data indefinitely, so they need to decide how long they plan to retain personal data and how it will be deleted. Just moving a file to a computer's recycle bin isn't good enough**.**

What do businesses need to do?

The Data Protection Commissioner has warned of a surge in consumer legal actions against non-GDPR compliant companies (Kennedy, 2017) so every organisation, big or small, should have an individual or team responsible for data management. In the run up to the GDPR taking effect next year, they must review their data protection procedures and plan how to make and keep the organisation GDPR-compliant. The review should map out questions like:

- What personal data do they hold?
- Have they collected this with the individual's consent?
- Is this data secure?
- Is it ever shared with third parties? If so, is there a record of this?

Following this, organisations need to identify any deficiencies in how they manage data and address them, ensuring that all staff who work with the data are informed.

Recommended sources for further information

- The GDPR and You, from the Irish Data Protection Commissioner, the first in a series of publications on GDPR.
- THE GDPR: A Guide for Businesses, from A&L Goodbody.

This article is general information, and does not constitute legal advice or analysis.

References

Castlebridge Associates (2017) 'Subject access requests: a data health check'. Available at: https://castlebridge.ie/products/whitepapers/2015/09/subject-access-requests-data-health check (Accessed March 23, 2017).

Edwards, E. (2017) 'Civil Service payroll system suffers further data breach', *The Irish Times*, 23 January [Online]. Available at: http://www.irishtimes.com/news/ireland/irish-news/civil-service-payroll-system-suffers-further-data-breach-1.2948177 (Accessed 16 March 2017).

European Commission (2016) 'EU-US Privacy Shield'. Available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf (Accessed April 3, 2017).

Kennedy, J. (2017) 'European consumer lawsuit tsunami will come in wake of GDPR', *Silicon Republic*. Available at: https://www.siliconrepublic.com/enterprise/gdpr-legal-tsunami (Accessed March 23, 2017).

Lonergan, K. (2017) 'Why the cloud makes the EU-US Privacy Shield meaningless', *Information Age*. Available at: http://www.information-age.com/why-cloud-makes-eu-us-privacy-shield-meaningless-123461178/ (Accessed April 3, 2017).