ICDL Foundation

SKILLS FOR DATA PROTECTION

Preparing workers to protect personal data

icdl.org

Contents

Executive summary

Data protection is an important topic, especially considering the implementation of the EU's General Data Protection Regulation and recent high-profile data breaches that have undermined public trust in organisations.

This position paper from ICDL Foundation highlights the importance of developing workers' skills for data protection.

Key takeaways

- **Data protection is not only important for Data Protection Officers.** Ordinary workers need to know how to handle personal data safely.
- **Workers who don't understand data protection are a risk to their employers.** The consequences of breaches of data protection rules can be costly to organisations, both financially and in terms of their reputations.
- **Acquiring skills for data protection in a structured way is better than hoping employees will figure it out for themselves.** Structured training that is verified by high-quality certification ensures that employees truly know how to safely handle personal data.

We think that there needs to be a concerted effort from policy-makers and employers at all levels to equip Europe's workforce with skills to handle data protection. To ensure the success of GDPR, everyone who processes personal data must understand how to do so safely and effectively.

Introduction

Data protection skills are not just the preserve of people in specialist roles, such as Data Protection Officers – they are crucial for all knowledge workers. Developing awareness, knowledge and practices around the protection of personal data can help individuals to preserve the reputation of their organisation and understand their own rights as data subjects.

In this position paper on data protection skills, we want to show that it is essential to ensure that all workers who process personal data have the opportunity to develop and demonstrate the skills to handle that data in a way that, first, protects data subjects, and second, prevents harm to their organisations.

Why is data protection important?

The topic of data protection has been in the spotlight recently, with the implementation of the General Data Protection Regulation (GDPR) in the European Union in May 2018 and the legislative work on the ePrivacy Regulation[1] that is ongoing at time of publication. While it has always been important to ensure that personal data is processed in a safe and secure way, the significant changes in regulation and oversight of data processing have pushed the subject to the fore.

Organisations that process data, including multinational businesses, small and medium enterprises (SMEs), non-profits, and governments, have had to work hard to comply with the requirements of the GDPR, or face the prospect of large fines of up to €20 million or 4% of global turnover[2], not to mention the risk of damage to their organisational reputation if a data breach occurs.

On top of this, the rise in importance of data for organisations, both large and small, brings increased risks and costs of data breaches[3]. New business possibilities from artificial intelligence driven by machine learning based on large-scale datasets of personal information will likely be a core element of the future economy in Europe and beyond[4], and this makes it more important than ever to ensure that the underlying data is adequately protected.

1 (European Parliament 2017)

2 Article 83, General Data Protection Regulation (European Union 2016)

3 IBM's 2018 'Cost of a Data Breach Study' calculated that the average cost of a data breach had risen to US$148 per lost or stolen record in 2018 from US$141 in 2017 (IBM and Ponemon Institute 2018)

4 (OECD 2017) (Bowles 2014)

Recent data breaches

There have been a number of recent high-profile examples of poor data protection. Most prominently, the Cambridge Analytica scandal, in which the personal data of 50 million Facebook users was captured and used without explicit consent to target political advertising caused outrage among many members of the social networking site and significant concern among regulators and authorities over the privacy policies and practices of Facebook and businesses operating on its platform.

In the particular case of Cambridge Analytica, people who logged into a quiz application created by an academic had information from their profiles and, significantly, from the profiles of their friends, collected and sent from the Facebook platform to the academic. He then passed on the data to Cambridge Analytica without informing users that he would do so[5]. Facebook policies at the time did not explicitly forbid this type of activity, and it is clear that the lack of a culture of, or concern for, data protection facilitated the breach.

Another significant example of a breach of data protection involved app maker, Ai.Type, which exposed 31 million customer records due to a misconfigured database[6]. In this case, the breach due to a lack of due care in configuring the database could likely have been avoided if data protection had been fully considered in planning the database.

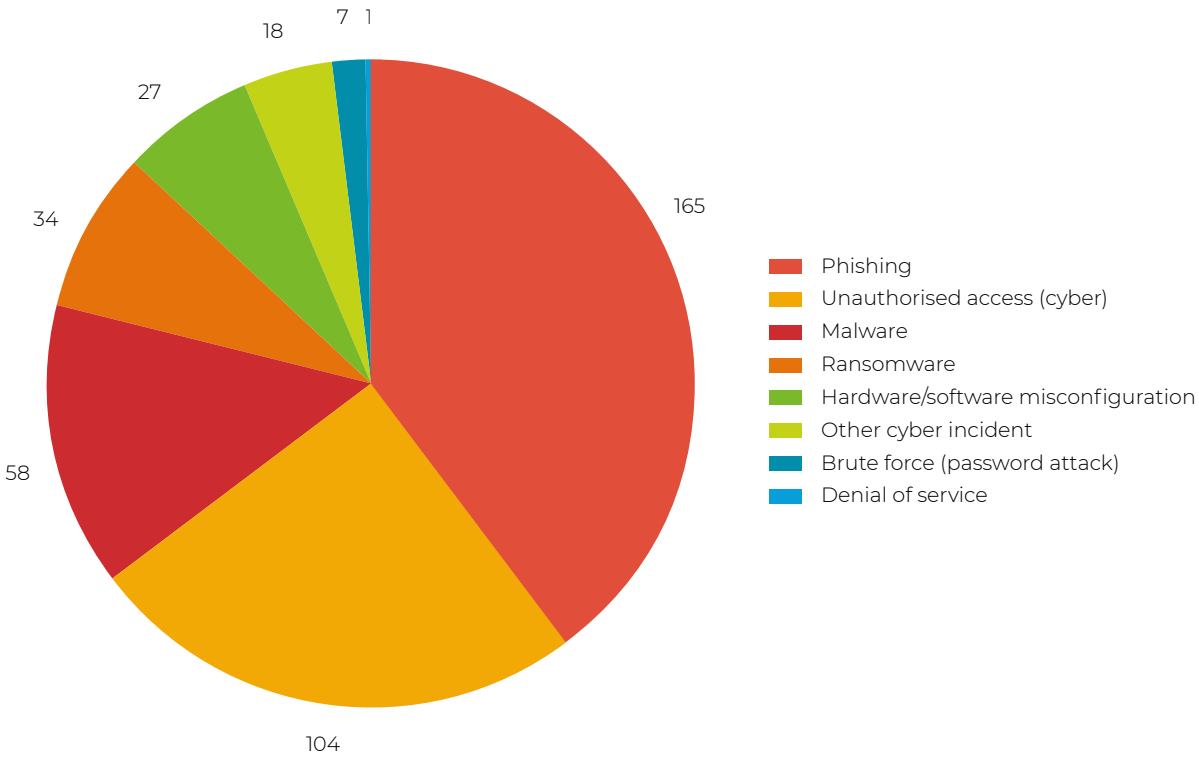
Mobile network, T-Mobile UK, also compromised customer data when sales staff sold upwards of half a million customers' records to data brokers[7]. What is key in these examples, is that they could be avoided easily by applying core data protection principles like data protection by design, or by instilling a culture of data protection throughout the workforce.

5 (Reuters 2018)

6 (Institute of Business Ethics 2018)

7 ibid

Reported data breaches by cause (UK, Q1 2018)



Source: Information Commissioner's Office, United Kingdom, 2018

A competence for all

While new or updated policies and the employment of specialised data protection officers are to be commended in strengthening data protection within organisations, these measures are inherently limited in their ability to prevent accidental or malicious data breaches by employees. It could be said that the weakest link for an organisation in ensuring the protection of personal data can be its employees.

The average employee has much easier and much greater access to personal data than ever before[8]. The centralisation of personal data for customers or prospective customers in Customer Relationship Management (CRM) software, and the prevalence of direct marketing tools for email and social media correspondence, facilitates both more efficient business practices – and more opportunities for something to go wrong.

In a summary of recent high-profile data breaches conducted by the Institute of Business Ethics[9] in the UK, internal breaches caused by employee error or malicious behaviour resulted in between 33 and 34 million data records being exposed. The breaches summarised included sensitive health insurance information from health insurance provider Bupa, employee information from Morrisons Supermarkets, and customer records from T-Mobile.

While a determined malicious employee can certainly expose personal data regardless of training or basic security measures, a large number of breaches occur by accident,

8 According to Gartner, the CRM industry is experiencing significant growth, with an expected 16% growth rate in 2018 (Gartner 2018)

9 (Institute of Business Ethics 2018)

either due to carelessness, technical error, or ignorance of how to protect data[10]. In short, if employees are handling personal data, it is clear that they need to know how to do so safely and why they need to do so securely.

A culture of data protection and the skills to implement it must permeate organisations that handle personal data. Simply expecting workers to just 'follow the policy' is insufficient. This is particularly apparent in situations where employees are expected to work in new scenarios. A policy written for one particular situation might not fit a novel situation, so the employees involved need the flexibility that a general competence in data protection provides to ensure that they do not risk causing a breach of personal data.

The perception and reality of skills

ICDL Foundation and its partners in Europe and Asia investigated the gap between peoples' perception of their digital skills, and the reality. We consistently found that people overestimated their abilities. In the studies, conducted in Austria, Denmark, Finland, Germany, Switzerland, Singapore and India, participants were asked to rate their digital skills in a number of areas. They were then were tested, using questions based on ICDL, to find out their actual abilities in those areas. Even in highly digitally developed countries like Singapore and Switzerland, participants routinely overstated their digital skills. 85% of participants in Switzerland thought they had good or very good skills for using the internet and email; only 34% actually performed that well. The clear unreliability of self-assessment of skills has a particular significance, and potential negative consequences, in a mission-critical area like data protection.

Developing the competence

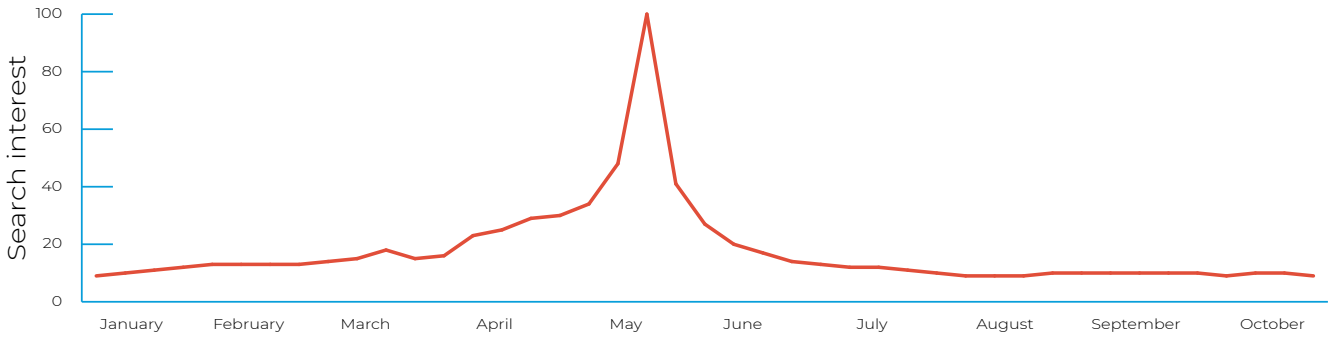
A quick search for the term 'GDPR' will show that there is considerable interest in learning how to comply with the regulation. Videos and 'how to' articles abound with advice. A small industry of 'data protection consultants' sprang up in the months before GDPR's implementation in May 2018[11]. However, it is unclear if this ad-hoc approach to developing competences for data protection is sufficient. The lack of any clear definition of which skills and knowledge are key for working with personal data safely means that there is a very real risk of important areas being overlooked. It is essential that there be a clear framework or structure that defines what skills ordinary workers need to have in order to protect personal data as they work with it.

Alongside ensuring that there is a clear structure that comprehensively covers the skills that are essential for data protection, it is vital that workers can show evidence of having

10 (Information Commissioner's Office 2018)

11 (Google 2018) Search interest is shown relative to the peak popularity of a search term, with 100 representing that moment. If the search interest is 50, then it is half as popular as it was when it peaked.

Worldwide search interest in 'GDPR' on Google



Source: Google Trends

these skills. In the area of digital skills, we have seen a big difference between actual measured skill levels, and self-assessed skill levels[12].

Beyond providing an incentive to complete training, certification also offers benefits to organisations. Under Article 83(c) and (d) of the GDPR[13], supervisory authorities setting penalties for infringements of the Regulation can take certain factors into account, including whether an organisation that is in breach of GDPR has taken steps to attempt to prevent it. While each situation should naturally be judged on the basis of its own facts, pro-actively making an effort to ensure that staff have a comprehensive understanding of how to protect personal data can only reflect well on an organisation. It can also make an organisation stand out from its peers by contributing to its credentials as a "secure" organisation if, for example, this is formally required by its customers.

We think that it is vital that skills be certified. However, it is essential that the right skills and competences are certified. In the area of data protection, all workers should be able to demonstrate that they have the skills and knowledge to understand the basic concepts of data protection, understand the rights of data subjects, implement policies and measures for data protection in their own organisations and in relation to their own work, and comply with relevant regulations.

To support this, we have developed our own certification on data protection, which is aimed at ordinary workers who have to handle personal data as part of their work. The certification has been developed with the input of subject matter experts from around Europe, and it attempts to ensure that these key areas are comprehensively covered[14].

12 (ECDL Foundation 2018)

13 (European Union 2016)

14 More information may be found at http://ecdl.org/about-ecdl/data-protection

Conclusion

When considering data protection, it is essential to remember that it is dependent on individuals to uphold it. As workers and citizens, individuals need to be able to understand how to protect their personal data, and the personal data that they are entrusted with at work, so that they can protect themselves and their organisations from the risk of a data breach. As online and offline services increasingly rely on data, transforming it into a key commodity that the world runs on, we have to ask how we can keep that data secure.

The lack of digital skills and competences is a very broad policy concern. At all levels, it is clear that Europe needs to invest in building a digitally skilled workforce so that it can, not only keep up with the pace of technological development, but can get ahead and remain competitive internationally. The cost of digital ignorance is high, but the cost of ignorance of data protection is particularly high. From election interference that threatens the democratic bedrock of our societies, to the personal cost of financial information or, often worse, deeply sensitive personal information being exposed and abused, we cannot afford ignorance of how to keep data safe.

To counter this ignorance, we believe that it is crucial for individuals and organisations to invest in developing an understanding of data protection that is both comprehensive and practical. We call for the recognition and promotion of programmes that facilitate this, and the inclusion of measures to develop skills for data protection in policy at all political levels.

Bibliography

BBC. 2018. BBC News: British Airways boss apologises for 'malicious' data breach. 7 9. Accessed 10 17, 2018. https://www.bbc.com/news/uk-england-london-45440850.

Bowles, Jeremy. 2014. Bruegel: Blog - The computerisation of European jobs. 24 7. Accessed 10 17, 2018. http://bruegel.org/2014/07/the-computerisation-of-european-jobs/.

ECDL Foundation. 2018. Perception and Reality: Measuring Digital Skills in Europe and Asia. Position Paper, Brussels: ECDL Foundation.

Erlich, Yaniv, Tal Shor, Itsik Pe'er, and Shai Carmi. 2018. "Identity inference of genomic data using long-range familial searches." Science.

European Parliament. 2017. Legislative Observatory Procedure File 2017/0003(COD). Accessed 10 17, 2018. http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en.

European Union. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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." Official Journal of the European Union L119/1.

Gartner. 2018. Press Release: Gartner Says CRM Became the Largest Software Market in 2017 and Will Be the Fastest Growing Software Market in 2018. 10 4. Accessed 10 17, 2018. https://www.ibm.com/developerworks/community/blogs/d27b1c65-986e-4a4f-a491-5e8eb23980be/entry/2017_CRM_Statistics_Show_Why_it_s_a_Powerful_Marketing_Weapon?lang=en.

Google. 2018. Google Trends. Accessed 10 19, 2018. https://trends.google.com/trends/explore?q=GDPR.

IBM and Ponemon Institute. 2018. 2018 Cost of a Data Breach Study: Global Overview. Traverse City, Michigan: Ponemon Institute.

Information Commissioner's Office. 2018. "ICO: Data security incident trends." Accessed 10 19, 2018. https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

Institute of Business Ethics. 2018. "Beyond Law: Ethical Culture and GDPR." Business Ethics Briefings, May.

Molteni, Megan. 2018. Wired: The Creepy Genetics Behind the Golden State Killer Case. 27 04. Accessed 10 17, 2018. https://www.wired.com/story/detectives-cracked-the-golden-state-killer-case-using-genetics/.

Newman, Lily Hay. 2018. Wired: How Hackers Slipped by British Airways' Defences. 11 9. Accessed 10 17, 2018. https://www.wired.com/story/british-airways-hack-details/.

OECD. 2017. Future of Work and Skills. OECD.

Reuters. 2018. Reuters Factbox: Who is Cambridge Analytica and what did it do? 20 03. Accessed 10 17, 2018. https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F.

icdl.org