This was my initial post starting the discussion:

Europe's GDPR laws define a level of data privacy that business and the IT professionals must comply with in order to protect data. As Brookshear and Brylow (2019: 249) state, however, “making an action illegal does not preclude the action”. The difficulties enforcing such a policy can be seen in an ongoing example between Facebook and the EU.

Facebook complies with the GDPR rules at their European centre in Ireland but does not comply with GDPR in the United States of America where there are less stringent data protection laws. Facebook transfers its European user's data to America. Until recently this was allowed under the Privacy Shield: an agreement that allows country's that don’t comply to GDPR to store European data (Verdict, 2020). However, as the gulf in standards has increased between the EU and the US, this agreement was ruled invalid in July. Facebook has been asked to stop transferring Europeans data to the US and in turn, Facebook has threatened to pull its services from the EU.

The BCS code of conduct state (BCS, 2020) “carry out your professional responsibilities with due care and diligence in accordance with the relevant authority’s requirements”. A computer professional following this code would want to consider who their relevant authorities are. It is interesting to note that the relevant authority's requirements are not necessarily the authority of the state the professional (Facebook staff) is operating in but maybe that of the users.

Brookshear, J. & Brylow, D. (2019) Computer Science An Overview. 13th ed. Harlow: Pearson Education Limited.

The British Computer Society. (2020) BCS Code of Conduct. Available from: https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/ [Accessed 28 Sept 2020].

Verdict. (2020) Facebook’s vow to pull out of Europe reflects EU-US data transfer divide. Available from: https://www.verdict.co.uk/europe-data-privacy-us/ [Accessed 28 Sept 2020].

To which our tutor Nawaz Khan replied:

“Facebook complies with the GDPR rules at their European centre in Ireland but does not comply with GDPR in the United States of America where there are less stringent data protection laws. “

Hi Adam,

It is a good point. It actually raises an old debate on 'law enforcement' vs 'ethical perspective'. I think organisations also need to follow Corporate and Social Responsibility frameworks.

Regards,

Nawaz

To which I replied:

Hi Nawaz,

Yes, it is interesting that you relate Data Protection and Corporate Social Responsibility.

CSR is a business framework that helps companies be conscious of the impact they have on areas of society and the environment and ethically conduct business.

CSR is often thought of going above and beyond the rule of law, there are however country's where CSR has been written into the law itself. China notably mandates CSR through law asserting "a company shall comply with laws and administrative regulations, conform to social morality and business ethics, act in good faith, subject itself to the government and the public supervision, and undertake social responsibility." (Lin. L, 2019).

In countries where CSR is non-mandatory, companies can look to the international ISO 26000 Social Responsibility standard for guidance on how to do the "right thing" (ISO, 2020).

By investing in Data Protection companies can contribute to the broader goal of Corporate Social Responsibility.

A case example of a good CSR response to data privacy came in 2009 when Heartland Payment Systems, a large payment service in the US, had its data breached. HPS went above and beyond the law, ignoring the advice of their own lawyers, and decided to focus on educating customers about what had happened and making the attack details public (McNutly, 2020).

In doing so HPS started a valuable dialogue that helped other companies understand how they too needed to protect themselves better. In the short term, HPS took a large financial hit, but eventually, the company was able to rebuild its reputation by showing its commitment to improving security standards.

References

ISO. (2020) ISO 26000 Social Responsibility. Available from: https://www.iso.org/iso-26000-social-responsibility.html [Accessed 10 Oct 2020].

Lin, L. (2019) Mandatory Corporate Social Responsibility? Legislative Innovation and Judicial Application in China. Available from: https://www.law.ox.ac.uk/business-law-blog/blog/2019/05/mandatory-corporate-social-responsibility-legislative-innovation-and [Accessed 10 Oct 2020].

McNutly , S. (2020) ISO 26000 The unusual couple: how data privacy and GDPR can advance CSR efforts. Available from: https://www.businesstimes.com.sg/asean-business/the-unusual-couple-how-data-privacy-and-gdpr-can-advance-csr-efforts-1 [Accessed 10 Oct 2020].

Jonathan Nathan provided the interesting comment:

It's interesting what you write about privacy shield, as I have had first-hand experience of this. Where I work, our legal team have recommended that we do not use any Software As A Service provided by US companies when data is not hosted in the EU (and explicitly regulated under EU law). They are particularly concerned over the fact that EU law requires notification of data breaches earlier than US law.

Here are comments I contributed to other discussions

Hi Man, Nawaz and Victor,

"I think the countries or cities outside EU should promote some regulations which is similar to the GDPR"

I agree with this comment from Man. It is interesting that as well as the regulations imposed by nation-states there are international standards that companies from other parts of the world can benefit from following.

The ISO (International Organization for Standardization) develop standards which are recognized and applied globally. ISO 27001 is a standard for IT management of employee details and third party data among other things (International Organization for Standardization, 2020). Adoption of this standard can be used to help demonstrate compliance with GDPR.

International Organization for Standardization. (2020) ISO/IEC 27001. Available from:

https://www.iso.org/isoiec-27001-information-security.html [Accessed 05 Oct 2020].

Hi All,

Yes, I think digital signatures are a great way to help recipients distinguish between sources of data.

They cannot however ensure that data will not be leaked.

GDPR does not specifically address the use of passwords but it says that data should be "Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures."

This requires businesses to prevent unauthorized access to personal data (Information Commissioners Office, 2020).

For high-risk data such as passwords, we decided that storing the data on paper was the most secure method.

Storing passwords for root account access physically means that there is no means to obtain them by hacking.

Storing the data physically also restricts access to the data making it harder for the data to be leaked.

Information Commissioners Office. (2020) Passwords in online services. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/ [Accessed 05 Oct 2020].

Hi Antonios,

This is a very informative post which provides a good overview of how a data breach should be handled in action.

I think that your suggestion that this event should trigger a review of IT processes is very correct. I think they should specifically look at their "process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing" (European Parliament, 2020: Article 32)

When looking at their cybersecurity analysis procedure another component(along with side penetration testing) they should look at is their vulnerability assessment procedure. A vulnerability assessment aims to use a range of tools and methodologies to identify vulnerabilities and threats (Rouse, 2020). Vulnerability assessments aim to uncover as many vulnerabilities as possible whereas a penetration test aims to find how such vulnerabilities could be exploited (Murashka, 2017).

A combination of vulnerability assessment and penetration testing should feed into their improved cybersecurity analysis procedure.

European Parliament. (2016) General Data Protection Regulation. Available from:

https://gdpr-info.eu/art-32-gdpr/ [Accessed 05 Oct 2020].

Murashka, U. (2017) Vulnerability Assessment vs. Penetration Testing: Know Who Is Who. Available from:

https://www.scnsoft.com/blog/vulnerability-assessment-vs-penetration-testing [Accessed 05 Oct 2020].

Rouse, M. (2020) vulnerability assessment (vulnerability analysis). Available from:

https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis [Accessed 05 Oct 2020].