Data security requirements under GDPR

Charles Russell Speechlys

Charles Russell Speechlys logo

Alexander Dittel

United Kingdom May 19 2016

BACKGROUND

Criminal liability of hackers and other online criminals has been part of UK law since the Computer Misuse Act 1990. At the global level, various jurisdictions have existing digital-crime related offences in one form or another. Notably, the Budapest Convention on Cybercrime signed in 2001, required countries acceding to it (which included the United States, Canada, Japan, South Africa, etc.) to criminalise various acts that are considered misuse of public networks and unauthorised intrusion into devices.

The increase in online activity involving financial elements in the 1990's brought about a natural growth in financial gain focused digital-crime in what was a rudimentary digital security environment. Further solutions were required. At EU level, the introduction of the Data Protection Directive in 1995 (Directive) legislated for the first major requirement to implement 'an appropriate level of security', which applied to all businesses inevitably processing personal data. Following this, the UK has adopted equally 'loosely worded' industry specific digital security requirements, for example, in public electronic communication networks and financial services industries.

The Directive required data controllers to put in place technical and organisational measures which would "ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected". Advising IT professionals on what this actually means is difficult, not least due to the rapidly changing state of art. In 1998, when the Directive was implemented into national law, the available computing power may have struggled with simultaneously running the operating system, applications and encryption software. The implementation of solutions would be costly in part due to these demands on hardware and in part due to the developing security software. In addition, the understanding of the ‘risks inherent in the processing’ was perhaps focused on any pecuniary damage that the data subject could suffer, rather than any distress. Indeed, more often the actual damage would not be pecuniary but non-material.

However, the landscape has changed since 1998. On the one hand, non-material damage has been making headwinds (Google v Vidal-Hall [2015]) and, on the other, the understanding of the value of data has shifted due to the increased potential of business analytics, as well as new techniques of fraud. This changing environment is addressed by the recently adopted General Data Protection Regulation (GDPR) but also in other legislation, such as the Network and Information Security Directive, which is expected to enter into force in August and will be subject to a 21 months’ implementation period.

SECURITY REQUIREMENTS UNDER THE GDPR

The new security requirements under the GDPR take into account the data protection authorities’ past experience and the new digital environment, in which cyber-criminals operate as businesses and trade personal data in underground data markets, where, for example, the credit card details of a Ukrainian citizen are worth $0.20 and those of a US citizen $2.00. Rather than carrying out a denial of service (DoS) attack, cyber-criminals would only forewarn the corporate victim of their attack and ask for a ransom to prevent it. Repeating this a thousand times each month with a 10% success rate leaves the cyber-criminal with a nice monthly income.

The GDPR requires that “Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk … account shall be taken in particular of the risks that are presented by processing … which could lead to physical, material or non-material damage.”

The GDPR helpfully spells out what processing may present risk of damage. This includes, processing that may give rise to discrimination, identity fraud, professional secrecy; processing where data subjects may be deprived of their rights or control over their data; processing that may lead to disclosure of racial, religious, genetic and other special categories data; evaluation of personal aspects, such as work performance, health, reliability or economic situation; processing of vulnerable persons’ data and processing on a large scale. In conclusion, risk of damage may result from most of the processing that will take place in a corporate environment. From a security point of view, risk of non-material damage may not be dismissed as negligible.

STEPS TO BE TAKEN

IT professionals often ask us what are the specific requirements which they must implement in their organisation? To their disappointment, the answer is often vague: “Carry out a privacy assessment, consider the risks and implement appropriate measures.” But let us look closer at what this means.

Carry out a detailed and objective privacy impact assessment setting out the type of personal data being processed and the processing operations and evaluate the risks, according to what the GDPR suggests may give rise to risk, as mentioned above. It is important to note that this exercise is aimed at personal data rather than data in general. Cyber-security (also referred to as “digital-security”) has been elevated to a leadership and management issue, rather than a matter simply for the IT department.This assessment should be probably led by compliance (or the Data Protection Officer, if you have appointed one) and should involve senior stakeholders from all departments, including, IT, HR, finance, legal, marketing and sales. If required, you may seek help from external advisers to guide you through the various stages of the assessment and to reach objective conclusions.

Based on your evaluation of the risks, select appropriate state of art technical and organisational measures that each of the stakeholders agrees will be effective and capable of being implemented within the organisation. When considering the measures, the business should bear in mind that cyber-risk has to be managed in the same way as anything else that can damage the business. The level of risk will dictate the balance of investment in mitigation against the risk. According to the GDPR, the measures may include, pseudonymisation, encryption, measures ensuring on-going confidentiality, integrity, availability and resilience of systems and services (also known as the “CIA triad/AIC triad” model that guides information security policies within organisations); measures of monitoring, regular testing/threat simulations and continuous evaluation of their effectiveness and an incident response plan including regular backups. If required, you may seek external help, perhaps from penetration testers (sometimes also referred to as “white hat hackers”, which may not necessarily be an appropriate term), for a vulnerabilities and resilience testing of your systems, ranging from hands-off assessment of your controls to a full “Red Team Exercise” where the testers will act as malicious attackers.

If you are stuck and genuinely feel that some of the measures should but cannot be implemented in your organisation to mitigate any proposed high risk processing, you should consult your data protection authority and not start processing before you have done so.

Implement appropriate security and organisational measures into your business operations. This step will require months of preparation and on-going announcements and raising of awareness culminating in the launch of the measures and the publication of easy to follow succinct policies which tell employees all they need to know in order to make the measures work.

But what specific technical and organisational measures may be required under the GDPR? The state of art has moved on since 1998 in terms of computing power and devices will now smoothly run any well-implemented encryption software in the background. The latest security software has real-time detection, prevention and remediation capabilities. The cost of implementation could be substantial, especially for SMEs with no in-house IT capabilities. However, there are a variety of solutions in the market and even a modest security package, which ought to be more cost-effective, will probably elevate your business to a much more appropriate level of compliance.

SO WHAT ARE THE REQUIREMENTS?

Please see below what we believe would be the minimum requirements for SMEs, not processing personal data as the core business. It should also be noted, that if your organisation, for example, only processes HR related personal data, the requirements may be limited to your HR processes, servers, personnel, etc. and all other data may be subject to less stringent security measures equal to the standards adopted in your industry.

Please note that the list below is based on assumptions and is intended for guidance only. It may not be relied on without carrying out a privacy impact assessment and obtaining security and legal advice. The GDPR does not specifically mention these measures, but on the basis of commonly adopted security measures and trends in enforcement action by data protection regulators, we can safely assume that these requirements are indeed a requirement. It is also important to mention that the requirements set out below are not new and will to a large extent also likely apply under the current legislation.

Minimum technical measures under the GDPR

Firewalls which are properly configured and using the latest software

User access control management by, for example, the UAC functionality in Windows. Please note, that in order to comply with the law, there should be no one person in your organisation with full access to all files and even your network administrator should have restricted access. In fact, it is recommended that the network administrator’s normal user account and his/her account with administrator privileges should be separated and only used when appropriate. This makes auditing and control of administrator actions much simpler. Failure to implement this measure has allowed for the Snowden incidents to happen

Unique passwords of sufficient complexity and regular (but not too frequent) expiry on all devices (including mobile phones) to defend against dictionary and rainbow table attacks. The UK government’s National Technical Authority for Information Assurance (CESG) has recently advised against forcing users to change their ‘complex’ passwords because this may lead to the recycling of old passwords, which may be already known to attackers, the need to note passwords down often on an exposed medium left near the device and users forgetting their passwords and being locked out, which leads to a loss in productivity

Regular software updates, if appropriate, by using patch management software

Timely decommissioning and secure wiping (that renders data unrecoverable) of old software and hardware

Real-time protection anti-virus, anti-malware and anti-spyware software

Encryption of all portable devices ensuring appropriate protection of the key

Encryption of personal data in transit by using suitable encryption solutions. This may include SSL and IPsec VPN connections which are appropriate for machine-to-machine connections, or PGP which is generally used for messaging, such as, e-mail. PGP or “Pretty good privacy” (around since 1991) has long been part of state of the art security. Nevertheless, if your organisation processes minimal amounts of personal data, encryption will not strictly be a legal requirement and organisations may achieve appropriate levels of security and comply with the law by other means

Implement secure configuration on all devices (including mobile phones)

Put in place intrusion detection and prevention systems

Data backup

Minimal organisational measures under the GDPR

Vet and train staff, contractors, vendors and suppliers on continuous basis, as individuals are often the weakest link

Insist on non-disclosure agreements prior to entering into formalised agreements

Provide training to staff on data processing obligations, identification of breaches and risks. Even with state of art security software you may not be able to prevent some breaches without having appropriately trained staff

Restrict staff access to personal data to those who need to know (also referred to as the “principle of least authority”)

Ensure physical security on premises including policy for staff to lock away their documents overnight in secure cabinets, and disposed of any sensitive printouts, which are no longer needed, by putting them in a confidential bin or through a cross cut shredder

Put in place a BYOD policy if you allow use of personal devices for work and

Implement a strict ban on the use of personal email for work purposes.

Other suggested commonly adopted security practices

Consider multi-factor authentication, especially for remote access. Without putting a burden on the employee, nowadays, the second authentication can be a fob plugged into the device or through the presence of a corporate mobile phone

Keep Wi-Fi passcode confidential and change it regularly to prevent creation of “evil twin” Wi-Fi access points. Generally, any WiFi access to the corporate network should use WPA-TKIP which is a centrally administered authentication method and grants access only to authenticated users, such as staff and

Implement delinquent web filtering to prevent access to hazardous URLs

In addition, the GDPR imposes the same data security requirements on data processor. Data controllers’ obligation to select data processors “providing sufficient guarantees” in terms of security will remain but the contractual obligations that the controller has to impose on its processor will focus on those that will “assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of … data subject's rights”.

Generally, we would recommend larger businesses to implement the ISO 27001 standards. However, given that the certification process can easily take up 4 – 12 months of staff and management time and prove to be quite burdensome, it may not be suitable if your personal data processing activities are minimal. On the other hand, these considerations may be outweighed by your clients’ requirement that you meet the ISO 27001 or ISO 27032 standards. SMEs should comply with at least the standards advocated for by the UK Government’s Cyber Essentials Scheme, ideally the “Plus” version, which includes external testing. However, SMEs that regularly deal with larger clients may well have to take the ISO route in order to remain competitive and satisfy their clients’ needs.

Finally, every organisation should consider taking out a cyber-security insurance policy. Insurers will demand a certain standard of security and may be unable to quote if the responses to their questionnaires show gaps in your security framework. A £5 million indemnity limit is common and it is yet to be seen if the insurance industry increases it to cover the potential €20 million fines, which data protection regulators will be able to impose from 2018. It is also worth noting that even if a policy is approved, it may not pay out if an incident was caused by failed controls, such as, an unpatched firewall. For this reason and the reasons set out above, if your organisation engages in processing of personal data on a large scale, its commitment to security should be nothing less than unrelenting.

CySure

CySure Limited

2, Printer's Yard, 90A The Broadway,
Wimbledon, London, SW19 1RD

D : +44 (0) 20 8412 1106 | W: www.cysure.net

CYBER ESSENTIALS IASME Consortium®