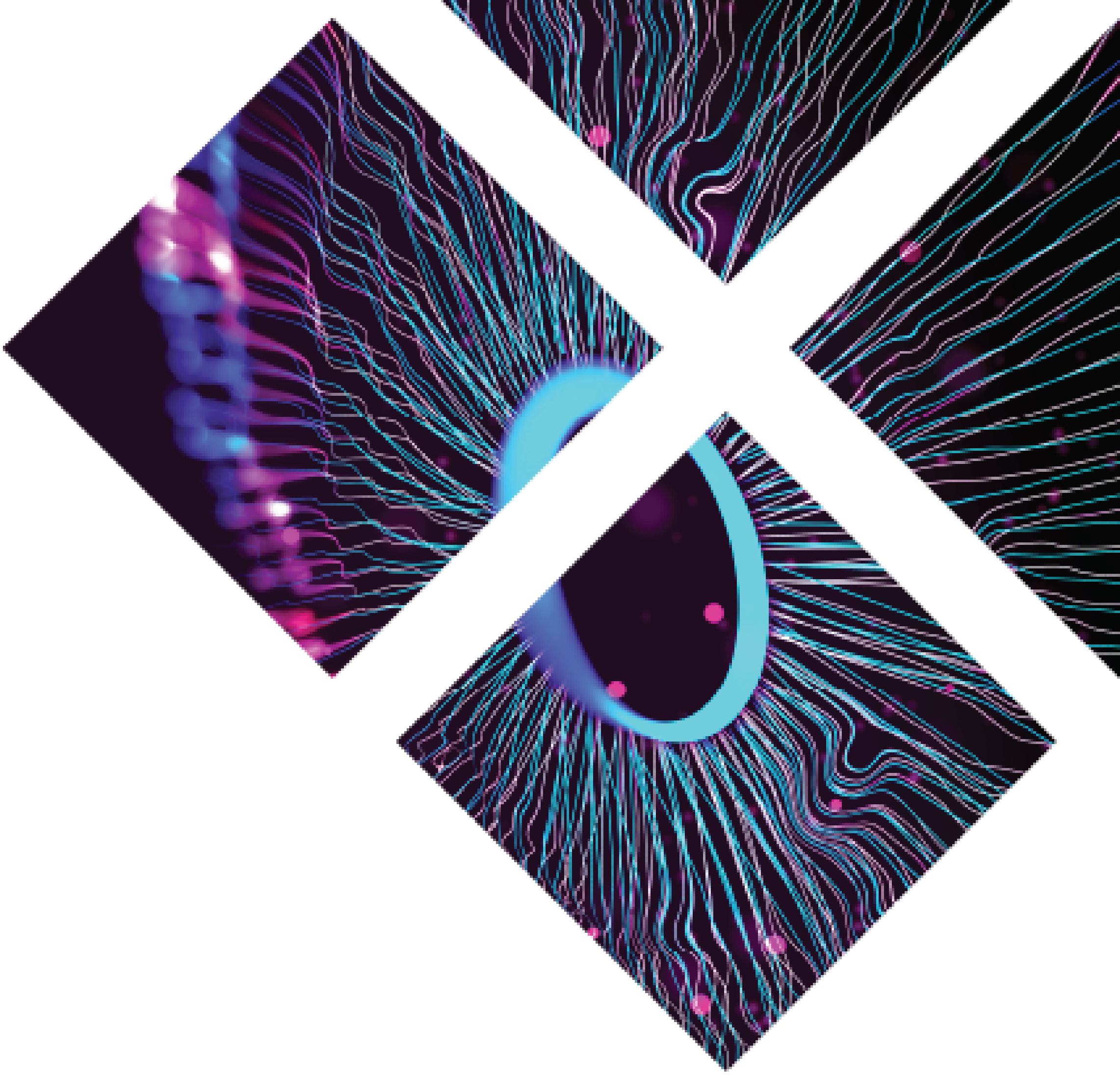


WHEN DOES THE GDPR APPLY TO DIGITAL TECHNOLOGIES?

WRITTEN BY KAVEH COPE-LAHOOTI

Gemserv

TABLE OF CONTENTS

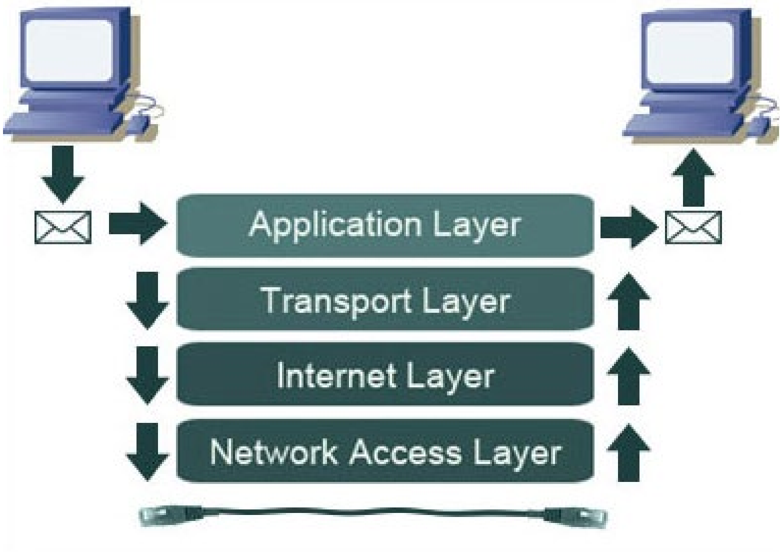
WHEN DOES THE GDPR APPLY TO DIGITAL TECHNOLOGIES?

As data processing and technological solutions offered to the market get more sophisticated and multi-layered, it is increasingly important to understand how and when GDPR applies to technology products and systems. Is your organisation getting it right?

This article analyses concepts such as data “processing” on organisations' software and hardware systems, with reference to the TCP/IP model (a widespread model for internet architecture), and how this may affect products vendors’ responsibilities under the GDPR. It demonstrates that more technology vendors (including software and hardware providers) may be inside the GDPR’s scope than would be immediately obvious – and such organisations should consider data protection controls appropriately for their systems.

WHAT IS THE TCP/IP MODEL?

One method to analyse how data is transmitted and stored within networks used by organisations involves using the Transmission Control Protocol/Internet Protocol (TCP/IP) model. The TCP/IP is a US Department of Defense model for describing the architecture of information exchanges on the internet. Typically, it consists of four ‘layers’ of communications, which include the following[1]:



These layers can be summarised as follows[2]:

- **Application Layer**: This is the highest layer and involves communications between computer programs and applications. This includes protocols such as HTTP for browser content. Typically, organisations controlling

[1] ITPRC (2008). HomeTCP/IPHow Encapsulation Works Within the TCP/IP Model. https://www.itprc.com/how-encapsulation-works-within-the-tcpip-model/
[2] GeeksforGeeks (2020). TCP/IP Model. https://www.geeksforgeeks.org/tcp-ip-model/

content at the application layer would involve developers for products like Microsoft Office tools and HR software.

- **Transport Layer**: This involves protocols used for transposing large data packets sent via the Internet Layer into usable information and allowing applications to talk to each other. The Transport Layer is typically used by most programs that use the Application Layer, including CRM systems, email or streaming services.
- **Internet Layer**: This layer involves sending data between 'A' and 'B', such as between two IP addresses. Telecommunications operators typically control the internet layer in national or global communications.
- **Network Interface Layer**: This is the lowest layer, which typically controls hardware for the physical transmission of data, including cables, devices, servers and mainframes. Typically, colocation data centre providers would maintain the network interface layer.

Which layers software or technology vendors use will depend on the functionalities of their systems and those they interact with. For example, expense management and CRM systems offered to the market will involve using the Transport and Application Layers, whereas cloud hosting providers will typically control the Network Interface and Internet Layers. This will also have a bearing on whether these systems "process" personal data.

WHAT IS DATA PROCESSING?

Understanding how the GDPR applies to various systems involves considering the definition of "processing". Article 4(2) of the GDPR outlines that processing essentially involves "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means" and lists activities such as "collection, recording, storage, disclosure by transmission", "data erasure" or "destruction". Organisations that conduct "processing", or provide systems that conduct such processing, are subject to the GDPR as data processor or data controllers.

Processing has been held by the European Court of Justice to cover activities such as storing a video recording on a hard disk of a system (Rynes judgement[3]), loading personal data onto a web page (Lindqvist judgement[4]) and providing the facilities to enable temporary storage and data "indexing" of online content (Google Spain judgement[5]). The GDPR also outlines that it applies not just to organisations performing processing, but also those that "provide the means for processing personal data" (Recital 18 of the GDPR) including "producers of products, services and applications" (Recital 78).

The effect of these definitions are twofold. Firstly, they imply that 'data processing' applies across all technologies – ranging from online software for transmitting and storing information, to the storage of videos on hard drives. This covers a variety of software and hardware products that technology vendors may have on the market. Secondly, that processing involves a wide definition – and so is likely to also apply to organisations providing such systems, as well as analysing or collecting the data itself. The implication of 'processing' such data would be that an organisation operating or providing these systems is considered within the GDPR.

[3] *Ryneš*, C-212/13, EU:C:2014:2428, paragraphs 23 and 25

[4] *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 25

[5] *Google Spain, Google Spain SL and Google Incoporated*, C-131/12, EU:C:2014:317, paragraph 28

WHAT ARE THE DATA PROTECTION IMPLICATIONS OF THE TCP/IP MODEL?

The implications of this wide definition of “processing” are that a variety of activities will constitute “processing” and therefore fall within the GDPR’s remit. In particular, returning to the TCP/IP Model, we can consider the following:

- **Application Layer**: Organisations providing solutions at the Application Layer are “data processors”. For example, providers of software such as Salesforce, Mailchimp, Oracle and others use the Application Layer for their systems and services. These involve both “storing” information and potentially “collection” of information, such as through data discovery or data scraping activities that software can be instructed to perform.[6]
- **Transport Layer**: Most products using the Application Layer also use the Transport Layer for communications and are likely to be “processing” data. Email clients, CRM systems and streaming products conduct Transfer Layer activities, such as controlling information to select and transfer as part of data retrieval, or requesting data in various formats (text, video, etc.). Organisations providing products such as Microsoft Outlook, Zoom or Wirecast that operate across the Transport Layer will thus be “data processors”.
- **Internet Layer**: Communications at the Internet Layer also involve the “transmission” of personal data, as they involve transporting it between systems (such as sending voice data and other media content across a mobile network). Moreover, organisations that operate the Internet Layer – telecommunications and broadband operators such as Vodafone, Virgin Media and others – typically have access to traffic and network data, which they can analyse as part of data processing.
- **Network Interface Layer**: Simply providing the infrastructure that allows data to be sent or stored is unlikely to be “processing”. Organisations that only provide the physical and infrastructural elements of communications, such as via operating co-located data centres without applications or managed services[7] are thus unlikely to be considered “data processors”.

Another method to distinguish activities that do not constitute “processing” can be made by a comparison to elements that have since been proposed, but not included, into the GDPR. For example, Germany Data Protection Authorities (collectively ‘DSK’) previously proposed introducing the concept of a ‘producer’, which would involve the “manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part” into the GDPR. Obligations proposed by the DSK for these organisations included responsibility for assisting the controllers and processors’ Record of Processing Activities and data breach notification obligations, as well as ‘privacy by design’ obligations[8].

However, the proposal was ultimately unsuccessful at the EU level, owing to a general reluctance to reopen the text of the GDPR. Nevertheless, the DSK’s analysis suggests that such “producers”, such as manufacturers of infrastructural systems or firmware, would not ordinarily be “processing” personal data under the GDPR, i.e., without some means of

[6] TechTarget (2021). TCP/IP. https://www.techtarget.com/searchnetworking/definition/TCP-IP

[7] Open Access Government (2019). Co-location data centres and privacy regulations. https://www.openaccessgovernment.org/data-centres-privacy-regulations/63028/#:~:text=in%20our%20centres.,Data%20Processing%20Agreement%20(DPA)

[8] Datenschutzkonferenz (2019, November). Independent German Federal and State Data Protection Supervisory Authorities: Report on Experience Gained in the Implementation of the GDPR. https://www.datenschutzkonferenz-online.de/media/dskb/20191213_evaluation_report_german_dpa_s_clean.pdf

involvement in the “collection, recording, storage [or] disclosure” of personal data; this fits with our above analysis of organisations’ responsibilities at the Network Interface Layer.

FINAL THOUGHTS

With reference to the TCP/IP model, this article has considered the application of the concept of “processing” to a variety of functions that technology organisations provide. In particular, it has shown that, apart from organisations providing physical or network access functionalities alone, a wide selection of software developers, cloud hosting providers and telecommunications operators will be bound by the GDPR’s provisions.

Vendors of these products should consider the application of the GDPR to their services, and how this will shape their risk profile. They could specifically consider:

- Organisations developing technology systems sold in the market should contemplate using web-facing positioning statement to outline their understanding of their processing activities, and ensure clients understand and apportion their responsibilities for their personal data.

- Product owners for such products and systems should examine the scope and controls at various layers that the product uses when transferring or storing data, as may need to be considered as part of a Transfer Impact Assessment or Data Protection Impact Assessment. Relevant privacy considerations can involve identifying what data can be ‘identified’ at each layer – such as the ability of metadata at the Transport Layer to reveal data subjects’ attributes based on call length, device IDs and location, regardless of whether Application Layer data is encrypted. Suitable security controls could range from using Virtual Privacy Networks at the Internet Layer, to antivirus software at the Application Layer.

- Vendors may also want to consider at which layers encryption should be introduced in their products. Transport Layer Security (TLS), can add another layer of encryption to data in transit, whereas Application Layer Encryption (ALE) can be enabled by product developers to encrypt particularly sensitive content.

Considering the above controls will help organisations developing technology products pre-empt any questions from users or clients, in addition to leveraging the reputational benefits from considering data protection at the various ‘layers’ their systems use when “processing” personal data. If in doubt, tech companies should take note – the application of the GDPR may be wider than it seems!

To find out more please contact:
Kaveh Cope-Lahooti
T: +44 (0)20 7090 1001
E: bd@gemserv.com
W: www.gemserv.com

London Office:
8 Fenchurch Place
London
EC3M 4AJ

Company Reg. No: 4419878

Gemserv

Certified B Corporation

INVESTORS IN PEOPLE
We invest in people Gold

ISO 27001 INFORMATION SECURITY MANAGEMENT

ISO 14001 ENVIRONMENTAL MANAGEMENT

ISO 9001 QUALITY MANAGEMENT

CYBER ESSENTIALS PLUS