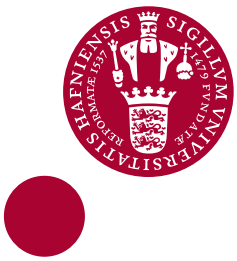

A Controller Without Control.

Embedded Artificial Intelligence – A Catalyst to Reconsider the Controller/Processor Relationship of the GDPR

Dahi, Alan; Corrales Compagnucci, Marcelo

Published in:
AI in eHealth

Publication date:
2021

Document version
Early version, also known as pre-print

Citation for published version (APA):
Dahi, A., & Corrales Compagnucci, M. (Accepted/In press). A Controller Without Control. Embedded Artificial Intelligence – A Catalyst to Reconsider the Controller/Processor Relationship of the GDPR. In M. Corrales Compagnucci, M. L. Wilson, M. Fenwick, N. Forgó, & T. Barnighausen (Eds.), *AI in eHealth: Human Autonomy, Data Governance & Privacy in Healthcare* Cambridge: Cambridge University Press. Cambridge Bioethics and Law

A Controller Without Control. Embedded Artificial Intelligence – A Catalyst to Reconsider the Controller/Processor Relationship of the GDPR[+]

Alan Dahi[*] and Marcelo Corrales Compagnucci[**]

Abstract In the past, AI-devices offloaded their processing to the cloud, clearly implicating the provider of the cloud as either a controller or a processor under the General Data Protection Regulation (GDPR). Increasingly, however, AI-driven processing is moving away from the cloud. Dedicated AI chipsets embedded in mobile clients and various edge devices now provide on-device predictions. A smart phone can screen for skin melanomas without sending any data to the cloud or app developer, and a bedside patient monitoring system can process locally in the hospital without sending any personal data to the device manufacturer. Such localized processing reveals underlying problems of how responsibility within data protection is allocated. For example, device manufacturers are typically deemed to fall outside the scope of the GDPR. This essay argues that the current understanding of the controller/processor framework is too narrow. This is demonstrated through various processing scenarios.

Keywords GDPR, controller, processor, household exemption, data protection-by-design, AI, fundamental rights, manufacturer, producer

1. Introduction

In times past, the web of actors processing personal data was neat and simple. You had a 'data subject,' the 'identified or identifiable natural person' about whom the information in question relates (Article 4(1) GDPR). You had a 'controller,' the entity who 'defines the means and purposes of the processing (Article 4(7) GDPR). Potentially, you had a 'processor' who processed personal data on behalf of the controller if the controller did not process personal data directly themselves but outsourced the task (Article 4(8) GDPR). If services had a digital component, the component itself was isolated and dealt with by one or two actors. Clouds were weather phenomena and the Amazon was located in South America.

Today, the web of actors involved in a typical processing activity is as dense as the Amazon rainforest. Apps and websites share your personal data with third-party advertising companies that create profiles on you to target their ads. A recent report by the Norwegian Consumer Council (NCC) observed that data was transferred to at least 135 different third parties involved

---

[+] This is a draft version. The final version will be available in *'AI in eHealth: Human Autonomy, Data Governance & Privacy in Healthcare'*, edited by Marcelo Corrales Compagnucci et al., forthcoming 2021, Cambridge Bioethics and the Law series, Cambridge University Press.

[*] Alan Dahi is a data protection lawyer and consultant based in Vienna, Austria.

[**] Marcelo Corrales Compagnucci is a Postdoctoral Researcher at the Center for Advanced Studies in Biomedical Innovation Law (CeBIL), Faculty of Law, University of Copenhagen, Copenhagen, Denmark.

in advertising and/or behavioral advertising by the 10 investigated Android apps.[1] The current 'List of Third Parties (other than PayPal Customers) with Whom Personal Information May be Shared' runs to 59 standard A4 pages when formatted in three columns of 'Party Name,' 'Purpose,' and 'Data Disclosed.'[2] Even a small family run web shop will typically use a number of service providers to run their business—managed email, web hosting, payment processors, logistics companies, and fulfilment services.

Similarly, devices that processed personal data were equally simple. Individuals may have used a personal blood glucose meter at home, regularly pricking their fingers for a drop of blood. The meter would record their blood sugar levels and the date and time of the recording. Future blood glucose monitors may rely on Artificial Intelligence (AI) and a non-invasive heartbeat scan instead of drawing blood, and they can help determine the optimal dose of insulin needed.[3]

The promise of such 'personalized medicine' is that medical treatment will be tailored to an individual's characteristics and thus more effective than the generalized approach used today. Its success rests heavily on AI and powerful number crunching capabilities.

Increasingly, AI is run on-device or in the periphery of the device, the so-called 'fog' or 'edge' computing. Fog networking utilizes computing resources closer to the end-users i.e., edge devices. The terminology employed is analogous to the Amazon metaphor. While the cloud is higher in the sky, the fog is much closer to Earth's surface (and end-users) and therefore much denser and covering wider areas. In other words, fog computing enables cloud resources to reside at the edge of the network as opposed to servers in a distant datacenter. For example, the sensors can collect the data, and instead of sending all the data collected to the cloud for further processing, they can shed some of their load to edge devices to perform certain (or all) processing and analyses such as filtering, prediction, classification, etc., where any AI algorithms can be applied to the edges, including machine learning (ML).[4]

This is in contrast to more distant processing in the cloud that has until now been the standard. The shift from the cloud to local processing is made possible by the development of specialized AI chips powerful enough to perform on-device 'inference', i.e., AI-driven prediction. The core of this article is an investigation into how this shift changes the data protection relationships of the processing taking place, in particular for the average at-home use of such devices outside of a professional setting. In order to be able to assess this change, however, we first need a high-level understanding of how AI is developed and works.

AI typically needs to be trained before it can be used—it 'learns' that given certain parameters a certain result may be expected.[5] With regard to training, an AI is like a lawyer (or doctor) who must first pass through standardized and standardizing education before being let

---

[1] Norwegian Consumer Council (*Forbrukarrådet*), 'Out of Control' (14 January 2020) <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/> accessed May 15, 2020, page 5.

[2] See PayPal, 'List of Third Parties (other than PayPal Customers) with Whom Personal Information May be Shared' (effective as of 1 April 2020) <https://www.paypal.com/uk/webapps/mpp/ua/third-parties-list> accessed 15 May 2020.

[3] Porumb, M., Stranges, S., Pescapè, A. et al., 'Precision Medicine and Artificial Intelligence: A Pilot Study on Deep Learning for Hypoglycemic Events Detection based on ECG' *Sci Rep* 10, 170 (13 January 2020). Bird J, 'Artificial intelligence paves the way for fully automated diabetes kit' *Financial Times* (March 10 2020) <https://www.ft.com/content/15f0123e-3b7d-11ea-b84f-a62c46f39bc2> accessed May 15 2020.

[4] Forti, S., Ferrari, G-L, Brogi, A., (January 2020). 'Secure Cloud-Edge Deployments, with Trust' *Future Generation Computer Systems*. 102: 775–788; Buyya, R., Sriram, S., (eds) 'Fog and Edge Computing: Principles and Paradigms', Wiley Series on Parallel and Distributed Computing (John Wiley & Sons, 2019).

[5] There are claims that some AI can learn *tabula rasa*, i.e., as an autonomous agent from a clean slate. In these cases, learning is based from first principles on experience and perception and not on any inherited or supplied knowledge about their environment. The first such claim was made by Google/DeepMind about their *AlphaGo Zero* program. See Silver D et al., 'Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm' *arXiv:1712.01815* (5 December 2017). See however Marcus G 'Innateness, AlphaZero, and Artificial Intelligence' *arXiv:1801.05667* (17 January 2018) for a critical assessment of whether *tabula rasa* claims are substantiated.

loose upon an unsuspecting public. The public sees the final, polished product that commands respect and inspires awe (regardless of actual capabilities, as a newly minted lawyer or doctor will surely attest to).

The manufacturer/producer will often be responsible for this initial training of the AI. Following training, the AI is ready to do its job and is embedded in the device. It may still improve over time, tweaking its knowledge to the specifics of its implementation, the same way we see how text auto-complete on our phones improves with use.

Once the AI is embedded, inference will ideally happen locally without any personal data transferred back to its alma matter, the producer. The benefits of such local-only processing are not only increased speed and accuracy. Fewer involved parties is also better for security and privacy. Moreover, local processing may permit the processing of health data and other special categories of personal data that enjoy extra protection under the GDPR, such as meeting one of the strict conditions for the collection of explicit consent of Article 9(2) GDPR from the user.[6]

Besides the myriad Internet-of-Things (IoT) devices that are finding their way into our homes and offices, local processing is also becoming more common with smart phones, which are well on their way to turning into tricorders of Star Trek fame. Smart phones can be used to analyze urine, screen for melanomas, predict neurological degeneration, and monitor general fitness. A smart phone can even be hooked up to a hospital bedside monitoring system that transforms our constant companions into a personalized nurse that keeps track of our individual medical histories.

According to the Office of the Australian Information Commissioner (OAIC), the health industry is the industry most vulnerable to breaches, followed by the finance industry—possibly because these industries deal with large amounts of data.[7] Bruce Schneier, a security technologist, argues that one of the main reasons for poor IT security is the lack of economic incentives: For example, '[h]ospitals' medical-records systems provide comprehensive billing-management features for the administrators who specify them, but are not so good at protecting patients' privacy [because] the economic considerations of security are more important than the technical considerations.'[8] Similarly, Ross Anderson, a professor of security engineering in the UK, argues that the failure to ensure appropriate security standards happens because people who are responsible for ensuring security are not the ones who suffer from the security failure.[9]

You may remark that the GDPR does impose fines of up to 2% of global annual turnover or 10 million Euro, whichever is greater, for a breach of data protection by design, and up to 4% / 20 million Euro where the Article 5(1)(f) GDPR principle of integrity and confidentiality is violated. However, these fines can only be levied against the implicated controller or processor (see Article 83 GDPR). And there's the rub.

The predominant opinion is that producers, i.e., entities that only manufacture the device and that do not (directly) process personal data themselves, are neither controllers nor processors; they are mere suppliers of devices to the controllers and processors that process personal data.[10] As the 2019 'Report on Experience Gained in the Implementation of the GDPR' by the German Data Protection Supervisory Authorities concludes:

---

[6] See e.g., European Data Protection Board, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications' (version 1.0 adopted on 28 January 2020), paras 70-71.

[7] Office of the Australian Information Commissioner, 'Notifiable Data Breaches scheme 12-month insights report' (13 May 2019) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/> accessed 15 May 2020.

[8] Schneier B, 'Economics and Information Security' *Schneier on Security* (29 June 2006) <https://www.schneier.com/blog/archives/2006/06/economics_and_i_1.html> accessed 15 May 2020.

[9] Anderson R, Moore T, 'The Economics of Information Security', 314 *Sci* 610 (2006).

[10] See e.g., Baumgartner U, 'Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen' in Eugen Ehmann, Martin Selmayr (eds), *Datenschutz-Grundverordnung* (C.H.Beck 2017), para 5; Bygrave L, 'Article 25. Data protection by design and by default' in Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler (eds), *The General Data Protection Regulation (GDPR) – A Commentary* (Oxford University Press 2020) 578; Hartung J, 'Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen' in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung/BDSG* –

> Controllers do not generally develop hardware and software themselves. They are largely reliant on available hardware and standard operating systems and application software. Monopolies and oligopolies often exist on the supplier side, as a result of which suppliers are able to dictate what products are used as well as the terms and conditions of that use. The GDPR's data protection by design/by default principles are geared to producers but do not impose any obligations on them in that capacity. The call for data protection by design/by default thus often comes to nothing if it is directed only at controllers.[11]

If it is indeed the case that a producer of a device that processes data only locally is neither a controller nor a processor, and this device is used for purely personal or household purposes by a natural person, any processing of personal data would fall under the 'household exemption' of Article 2(2)(c) GDPR. This would push processing by such 'local only' devices, when used for purely personal or household purposes, outside the scope and protection of the GDPR.

We posit that the criterion of local or remote[12] processing is inadequate to distinguish whether processing is covered by the GDPR. As will be explained in the following sections, this 'producer dilemma' highlights an underlying problem within the GDPR that AI is only exacerbating—that of data protection responsibility within the controller/processor framework. The methodology we use combines a systematic legal dogmatic analysis with a teleological interpretation of EU court decisions. After this introduction, section 2 compares different hypothetical scenarios to show that the current understanding of the GDPR's controller/processor framework leaves unjustified gaps that need to be filled. Section 3 concludes.

2. Data protection responsibility – assessing the controller/processor framework and the household exemption

A data protection lawyer may know the feeling. You are assessing a data processing activity and find good reasons to classify your client as either a controller or as a processor. Guidance issued by the Article 29 Data Protection Working Party, a European body representing the national supervisory authorities for data protection, is too vague to lead to a 'right' decision.[13] Being left in the lurch, the decision on whether to classify as a controller or a processor will depend on what is more beneficial for your client. Occasionally, you may even find yourself in the bizarre situation where no actor is responsible for data protection, for example because the household exemption of Article 2(2)(c) GDPR seemingly applies, which excludes from the scope of the GDPR processing by a natural person for purely personal or household purposes.

Remembering that 'the **first and foremost role of the concept of controller** is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to **allocate responsibility**,'[14] you start to question whether the current understanding of the controller/processor framework is viable and think of further scenarios that call for a revised understanding of the framework.

Kommentar (C.H.Beck 2018, 2nd ed) para 12; Hartung J , 'Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen' in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung/BDSG – Kommentar* (C.H.Beck 2018, 2nd ed) para 13.

[11] Independent German Federal and State Data Protection Supervisory Authorities (*Datenschutzkommission*), 'Report on Experience Gained in the Implementation of the GDPR' (November 2019) 15.

[12] 'Remote' meaning processing by another party besides the data subject, regardless of whether the data is sent to that party or that party accesses the data on-device.

[13] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010).

[14] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010) 4. See also *Google Spain and Google*, C-131/12, EU:C:2014:317, para 34, which speaks of 'effective and complete protection of data subjects'.

This section assesses four such scenarios, all tied to the household exemption, against the goal of allocating responsibility.

2.1. The household exemption

Under the household exemption of Article 2(2)(c) GDPR, the GDPR does not apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity.'

This does not mean that all processing somehow connected to purely personal or household activities falls outside the scope of the GDPR. According to Recital 18 GDPR, the GDPR still 'applies to controllers or processors which provide the means for processing personal data for such personal or household activities'—but the exact frame of this scenario is surprisingly unclear. The European Data Protection Board (EDPB) guidelines on connected vehicles, which discuss such processing, reference Recital 18 GDPR but remain equally vague and merely rephrase the law without offering interpretive guidance:

> [While] the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, it does apply to controllers or processors, which provide the means for processing personal data for such personal or household activities (car manufacturers, service provider, etc.).[15]

The guidelines provide examples, but they are of local processing only, such as the unlocking of a car using locally stored biometric data.[16] As such, even the examples fail to add anything of substance to the understanding of the household exemption.

It is clear from the wording of Article 2(2)(c) GDPR that it is processing of a personal or household nature *by* a natural person that is outside the scope of the law. The processing of a natural person's personal data by an enterprise, a term used in this essay to cover a legal or natural person that does not process within the household exemption, is of course within the scope of the GDPR—and of course even if requested by a natural person for their own personal or household purposes. Indeed, this is one of the main areas where the GDPR applies. Consequently, only purely local processing by the data subject without any external transfer of, or access to, the personal data can in any way fall under the household exemption.

The next sections set out to investigate which scenarios Recital 18 GDPR intends to capture.

2.2. The household exemption: remote processing by an enterprise

The wording of Recital 18 GDPR entertains the possibility that enterprises 'provid[ing] the means for processing personal data for such personal or household activities' are controllers or processors. This understanding is repeated by the EDPB in its guidelines on connected vehicles, but without explaining what 'provid[ing] the means' actually denotes.[17] In order to conceptualize what may be meant, we now turn our focus to conceptualizing household exemption scenarios where an enterprise may be either a sole controller, a processor, or even a joint controller together with the data subject.

The enterprise as sole controller. Where the enterprise takes the role of sole controller, the GDPR's standard protection applies. The data subject can exercise their rights of information (Articles 13 and 14 GDPR), rights of access (Article 15 GDPR) and rectification (Article 16 GDPR), the relevant rights surrounding automated individual decision-making

[15] European Data Protection Board, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications' (version 1.0 adopted on 28 January 2020), para 73.
[16] European Data Protection Board, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications' (version 1.0 adopted on 28 January 2020), para 70.
[17] European Data Protection Board, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications' (version 1.0 adopted on 28 January 2020), para 73.

(Article 22), and others. The data subject also has explicit legal remedies against the controller under Chapter VIII GDPR, such as the right to lodge a complaint (Article 77 GDPR) or seek compensation (Article 82 GDPR). Finally, the data subject is also indirectly protected by virtue of the controller's obligations listed in Chapter IV GDPR, including that of data protection by design and by default (Article 25 GDPR), and also through the GDPR's general processing principles of data minimization, purpose limitation, etc., as provided for under Article 5 GDPR. The protections apply because under the clear wording of Article 2(2)(c) GDPR ('by a natural person'), it is only the data subject's *own* processing that falls outside the scope of the GDPR.

The enterprise as processor. Where the enterprise takes the role of processor, however, the situation is not as clear. For one, a data subject's rights are only valid against the controller. For another, not all GDPR obligations apply equally to controllers and processors. Data protection by design and by default, Article 25 GDPR, for example, mentions as the obliged party only controllers.[18]

Furthermore, the scenario of an enterprise taking the role of processor would in effect lead to a 'controllerless' processing situation:

Imagine a sleep monitoring device that is used for personal sleep tracking. It tracks your various sleep phases and sleep quality. It plots your sleep quality against your self-reported emotional state, the foods you ate, the amount of daylight you were exposed to during the day, and the amount of physical activity you enjoyed, all in order to recommend behavioral changes and make predictions about the future quality of your sleep. The data is processed remotely at the device producer and the results are then sent back to the device itself or to your phone. On an abstract level, you as the user will collect your own personal data. You will send it off to the producer and the producer will send you the results. In other words, the producer (henceforth 'enterprise')[19] will process the data on behalf of you, the data subject.

This 'processing on behalf' is at the core of the Article 4(8) GDPR definition of a processor: 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.' The only still-required element in our scenario is that the end-user of the sleep tracking device is not only a data subject but also the controller of the processing.

Article 4(7) GDPR defines the controller as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.' 'Determines', according to the Article 29 Working Party, is control over the means and purposes of the processing. 'Control' may result either from a) explicit legal competence (typically through a legal obligation to process, such as mandated by law), b) implicit legal competence (namely being naturally attached to the functional role of the entity processing the data, such an employer towards the employee), or c) simply boots-on-the-ground factual influence.[20]

The purpose of investigating where control rests is to appropriately allocate responsibility for the processing to where decisions about the processing are actually taken.[21] This responsibility is also reflected in how other languages name the controller. Examples are '*Verantwortlicher*' in German, '*responsable du traitement*' in French, '*responsabile del trattamento*' in Italian, '*responsible del tratamiento*' in Spanish and '*personuppgiftsansvarig*' in Swedish.

---

[18] Though certain obligations apply indirectly through the obligations imposed by the controller on the processor through Article 28(1) and (3) GDPR. See also European Data Protection Board, 'Guidelines 4/2019on Article 25 Data Protection by Design and by Default' (adopted 13 November 2019), paras 38 and 85.

[19] 'enterprise' is also defined in Article 4(18) GDPR as 'a natural or legal person engaged in an economic activity'. For the sake of simplicity, 'enterprise' is used in this paper accordingly to distinguish between a data subject falling under the household exemption and other relevant entities, including producers, manufacturers, etc.

[20] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010) 8 et seqq.

[21] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010) 8 et seqq.

With regard to the sleep tracking device, and indeed to most 'modern' services one might use for personal or household purposes, only implicit legal competence and factual influence are plausible determinators to allocate responsibility for the processing. It is hard to argue that the 'implicit competence' of the user of a service is to (solely) determine the purposes of the processing and that the service simply follows the user's instructions. Rather, the enterprise presents the end-user/data subject with terms of service that need to be accepted. The data subject can choose whether to accept the terms and use the service, but they cannot shape the service beyond the scope that the enterprise offers. Therefore, not only does any 'implicit competence' rest more with the enterprise than with the data subject, but also any 'factual influence' because of the enterprise's inherent ability to affect the processing and update the terms of service. It follows from this overwhelming influence that the enterprise should be deemed to be responsible for the processing and not the user—and consequently that the enterprise is not a mere processor.

Even if we were to extend the sleep tracking service to include a social sleep platform on which users can directly share, edit, tag, and delete personal data, the functionality itself is limited to what is made possible by the enterprise, who can add or remove such features as they wish. This does not give enough control to the user to elevate them to the role of sole controller.

Thus, the enterprise as processor scenario would give us a paradoxical 'controllerless' situation—paradoxical because a processor needs, by definition, a controller on whose behalf it processes personal data. Moreover, while conceptually possible that a controller and the data subject may be the same person, such as when a sole proprietorship processes personal data about itself, the whole conceptual structure of the GDPR breaks down when the two actors are one and the same.

In contrast to the private law concept of contracting with oneself, such as found in Section 181 of the German Civil Code, which prohibits an agent from 'enter[ing] into a legal transaction in the name of the principal with himself in his own name or as an agent of a third party,'[22] in data protection there is no agent/principal relationship for a data subject who is simultaneously a controller. As such, a data subject would be not only be in fact identical with the controller, but also *legally*, so that the data subject and the controller would be logically unable to contract / enter into a data protection relationship with each other. None of the rights granted a data subject against a controller need to be exercised, let alone enforced, where the controller and the data subject are one and the same.

That being said, at least with services where the user can shape to a certain extent the processing within the boundaries of what the producer offers, the user undeniably exercises a certain degree of control. Controllership is not an all-or-nothing issue. Article 4(7) GDPR permits a joint determination of the means and purposes of the processing, which leads us to investigate the possibility of joint controllership between the enterprise and the data subject.

The enterprise and the data subject as joint controllers. According to Article 26 GDPR, '[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.' At first glance, the user of a service and the enterprise may indeed, in certain situations, be regarded as joint controllers, as each can determine, albeit to a different extent, the means and especially the purposes of the processing. It does not matter that the user is in a weaker position because the level of influence between the two need not be equal. Both the Article 29 Working Party and the Court of Justice of the European Union (CJEU) have acknowledged that 'joint determination may take different forms and does not need to be equally shared.'[23] Advocate General Bobek of the CJEU even commented in his Opinion on

[22] Civil Code in the version promulgated on 2 January 2002 (Federal Law Gazette [*Bundesgesetzblatt*] I page 42, 2909; 2003 I page 738), last amended by Article 4 para.a5 of the Act of 1 October 2013 (Federal Law Gazette I page 3719).

[23] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010) 19. See also *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, para 39.

Fashion ID that the broad understanding put forward by the CJEU in the recent cases *Wirtschaftsakademie* and *Jehovan todistajat* makes it:

> difficult to see how normal users of an online (based) application, be it a social network or any other collaborative platform...would not also become joint controllers. A user will typically set up his account, providing parameters to the administrator as to how his account is to be structured, what information he wishes to receive, on what subjects and from whom. He will also invite his friends, colleagues and others to share information in the form of (often quite sensitive) personal data, via the application, thus not only providing data concerning those persons, but also inviting those persons to become involved themselves, in this way clearly contributing to the obtaining and processing of personal data of those persons.[24]

This is not hyperbole. Even though in *Wirtschaftsakademie* the Court did comment that 'the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network,'[25] a couple of paragraphs later, the Court gives a caveat by indicating that a user will be a (joint) controller where they take part in determining the purposes of the processing by defining parameters of the processing.[26] Advocate General Bobek's concern about expanding joint controllership to 'normal users' is justified.

Applying the reasoning of *Wirtschaftsakademie* and *Jehovan todistajat* to our sleep tracking device case, the data subject may very well be elevated to a controller insofar as they determine to a certain extent the processing operation—or, as the Court put it in *Wirtschaftsakademie*, 'ha[ve] an influence on the processing.'[27] By deciding when to use the device and tailor it to their needs, the user would be deemed to have an influence on the processing—at the very least whether it should take place or not.

However, we agree with Advocate General Bobek who highlights the problem of the Court's reasoning by following it to the extreme to include all parties that make a processing possible, including the Internet service provider.[28] Intuitively, he says, we reject broadening the scope to such an extent.[29]

Similarly, assigning joint controllership between a user of a service and the provider, simply because the service grants the user a certain degree of leeway in shaping the experience of the service, is wrong. Elevating the data subject to the role of (joint) controller hollows out the GDPR's differentiation between roles:

For one, joint controllership requires an agreement between the parties about the allocation of their obligations under the GDPR (Article 26(1) GDPR). Again, quoting Advocate General Bobek in his Opinion in *Fashion ID*:

> First, [the proposition of concluding contracts] is completely unrealistic, taking into account the dense web of formal, standard contracts that would have to be signed by any kind of party, including, most likely, a number of normal users. (…) Second, the application of valid legislation, and the allocation of responsibility it provides for would be made conditional upon private agreements, to which third parties seeking to enforce their rights might not have access.[30]

For another, even if one were to argue that the data subject as controller would not be required to enter into any such contracts because of the household exemption, this would still

---

[24] Opinion of Advocate General Bobek, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, para 73.
[25] *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, para 35.
[26] *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, para 39.
[27] *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, para 36.
[28] Opinion of Advocate General Bobek, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, para 74.
[29] Opinion of Advocate General Bobek, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, para 75.
[30] Opinion of Advocate General Bobek, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, para 86.

require some sort of fictious agreement between the data subject and the enterprise because the enterprise would still be subject to the obligation. This problem exists regardless that the Court in *Wirtschaftsakademie* held that:

> the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.[31]

In conclusion, most 'modern' services give the user some degree of control over the processing. This 'control,' which should rather be seen as a feature of the service and not as proper control, is in our view insufficient to disrupt the assignment of roles between data subjects, controllers, and processors, and assign to the data subject responsibility for the processing—in particular when this responsibility would include requiring entering into joint controllership and data processing agreements.

Rather, as will be shown below, processing by AI implicates a level of control that can shift responsibility to the device manufacturer by raising them to the role of controller or processor. This shift can happen regardless of whether the data is processed locally or remotely.

2.3. The household exemption: local processing by a data subject

The enterprise as producer. As mentioned in the introduction, it is common opinion that the GDPR does not extend to producers. This understanding rests to a large extent on Recital 78 GDPR, which reads:

> When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, *producers* of the products, services and applications *should be encouraged* to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.[32] (Emphasis added).

However, the definition of 'controller' does not require that a controller processes personal data itself but only that the controller determines the means and purposes of any processing.[33]

Such a literal interpretation permits the inclusion of device producers within the definition insofar as their downstream influence is so great that they still decide the 'means and purposes' of the processing even when the device and personal data are no longer in their hands. The definition of controller is such that it does not even require processing by a processor. It is enough that any downstream processing occurs, for example by the data subject, regardless of whether the data subject themself falls under the household exemption. In *Jehovan todistajat,* the Court also held that nothing in the law 'supports a finding that the determination of the purpose and means of processing must be carried out by the use of written guidelines or instructions from the controller.'[34] A factual determination appears sufficient.

---

[31] *Wirtschaftsakademie Schleswig-Holstein,* C-210/16, EU:C:2018:388, para 43.

[32] See e.g. Independent German Federal and State Data Protection Supervisory Authorities (*Datenschutzkommission*), 'Report on Experience Gained in the Implementation of the GDPR' (November 2019) 16.

[33] At least with regard to joint controllership, the CJEU has held that not each controller needs to have access to the personal data concerned: *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, para 38.

[34] *Jehovan todistajat,* C-25/17, EU:C:2018:551, para 67, albeit with regard to the GDPR's predecessor, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The definition of 'controller' did not change between the two laws.

Moreover, this understanding is not contradicted by a systematic approach and is supported by a teleological interpretation—the teleological approach being 'the characteristic element in the [CJEU's] interpretative method.'[35] The teleological method looks to the purpose behind the norm, whereas the systematic method looks to the how the norm itself fits within the overall structure of the law—and even the act itself within the overall legal system.

Systematically, the definition of 'controller' needs to mesh with the other provisions of the GDPR that use the term. The GDPR assigns different rights and obligations to the different data protection actors; these rights and obligations are sometimes limited by qualifying elements.

For example, the rights to information (Articles 13 and 14 GDPR) assume that personal data will be 'obtained,' and the right to access (Article 15 GDPR) obliges the controller to 'provide' a copy of the personal data being processing. Coming from a literal interpretation, the rights to information do not necessarily mean that the controller needs to directly obtain the data – simply that they are obtained by a party that processes them. On the other hand, the controller must 'provide' a copy of the personal data under the right to access. The term 'providing' would seem to indicate a more active role by the controller and in particular that the controller has access to the personal data. However, a looser reading of the term would be satisfied where the controller somehow enables the data subject to have access to their personal data.

Systematically, it is difficult to come to a firm conclusion. However, when supplemented with the teleological approach, it becomes clear that pure device manufacturers should fall under the scope of the GPDR, for the purpose of differentiating between the different data protection actors is to clearly assign data protection rights and responsibilities for any processing activities undertaken. The more complex the web of actors involved in a processing activity, the more important it becomes to be able to pinpoint responsibility and prevent the pointing of fingers, passing of blame, and failure of rights.

Within the trifecta of controller, processor, and data subject, the GDPR recognizes the controller as the entity with the utmost responsibility (see also Article 24 GDPR). The controller can outsource its processing to a processor, but it still remains ultimately responsible for the processing—regardless of the provisions within the GDPR that explicitly state this, such as Article 82(2) GDPR,[36] but already from a teleological perspective. A controller could easily escape its obligations by outsourcing the processing to another entity were this not the case. The processor is also responsible, but only within those specific obligations the GDPR assigns to it,[37] and in a relatively standard legal relationship as the controller's contractor. Finally, the data subject, too, is of course responsible—but only in regard to exercising common sense as 'an average consumer who is reasonably well informed and reasonably observant and circumspect.'[38] The data subject must be able to assume that market actors are generally compliant—our market economy and legal system is to a large extent trust based.[39] From a practical perspective, a data subject will not be able to conduct any thorough due diligence on the actors it engages with. This trust extends from buying an apple at a supermarket and trusting that it is fit to consume, to providing personal data to a hospital for the purpose of being treated and trusting that the data will be handled in accordance with data protection and other laws and not be sold for profit or carelessly disclosed to nosy neighbors. Such an assumption is also reflected in various obligations of data protection law that controllers are subject to, for example data protection by design and by default in Article 25 GDPR, but also in general sales law. By way of example, Section 434 of the German Civil Code declares that a 'thing is free from

---

[35] Fennelly N, 'Legal Interpretation at the European Court of Justice' 20(3) *Fordham International Law Journal* [1996] 656, 664.

[36] Article 82(2) GDPR: 'Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.'

[37] See Article 82(2) GDPR.

[38] *Gut Springenheide and Tusky*, C-210/96, EU:C:1998:369, para 31.

[39] See eg Castaldo S, *Trust in market relationships* (Edward Elgar Publishing 2017).

material defects if it is suitable for the customary use and its quality is usual in things of the same kind and the buyer may expect this quality in view of the type of the thing.'

On a more abstract level, the GDPR follows two goals, as noted in Article 1(1) GDPR: 'the protection of natural persons with regard to the processing of personal data' on the one hand and facilitating 'the free movement of personal data' within the European Union on the other. Clearly determining responsibility and closing any gaps in the law supports the goal of protecting natural persons—and by building data subject trust in a functioning data protection regime, also encourages the free movement of personal data within the Union. Without knowing anything about data protection in Ireland, a German resident will not be concerned that the controller responsible for their personal data is established in Ireland and will be happy to engage with the controller—at least in theory.[40]

Key to any scenario where a producer is subject to the GDPR, however, will be a sufficiently developed AI that processes personal data. Until the first AI is recognized as having legal capacity, it is clear that AI itself cannot be a controller. But its creator can be—and crucially at a stage that does not lead to employing infinite regress.

This reasoning can best be demonstrated when comparing processing by a traditional dumb device, such as a sleep tracker that merely records your heart rate, breathing, and brain waves, with processing by our AI-powered sleep tracker (which, for the purposes of this sub-section, now processes all personal data locally only). The smart sleep tracker does more than record – it analyses, assesses, learns, and provides an inference.

A dumb sleep tracking device does not have any level of autonomy. It processes personal data in a fully predictable input-output fashion subject to the user's instructions. A smart sleep tracker, on the other hand, processes personal data without instructions in the typical sense of the word. It provides output independently of the user's instructions. A clear example is that of a self-driving car. While the destination will be given to the car, just as to a cab driver, the actual driving, adhering to traffic laws, and the route, will be decided upon by the car. It may also suggest, based on advertising it receives on the way and the passengers' preferences, to stop at certain venues.

Moreover, the nature of AI is such that inferences may be unexpected and even unexplainable by the AI's developers. One poetic example of such 'behavior' was the historic Go match between AlphaGo, a Go-playing AI developed by the London-based and Google owned firm DeepMind, and South Korea's Lee Sedol, one of the world's best Go players. For the first time, an AI beat the world's best human at a game that is much more complex than chess and where computer domination was deemed to still be years away. In game 2 of the match, 'the Google machine made a move that no human ever would. And it was beautiful… the move so perfectly demonstrated the enormously powerful and rather mysterious talents of modern artificial intelligence.'[41]

The level of autonomy exhibited by a sufficiently developed AI means that by embedding the AI, the producer effectively decides how personal data will be processed downstream, and to a large extent independently of the user. While a user may be able to exert some influence within the possibilities permitted by the device, this is analogous to how a user of an online service can freely choose from the features provided by the service provider.

As explained above, under the current understanding of the controller/processor framework, the GDPR's protections do not exist in situations where the household exemption applies. This is because the local-only processing of the personal data by a natural person for purely household or personal purposes means that there is no controller or processor that falls under the GDPR, because device producers are excluded. Without an entity to exercise their rights

[40] See to the difficulty of litigating data protection in Ireland: Vinocur N, 'One country blocks the world on data privacy' *Politico* (25 April 2019) <www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/> accessed 15 May 2020.

[41] Metz C, 'In Two Moves, AlphaGo and Lee Sedol Redefined the Future' *Wired* (16 March 2016) <www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/> accessed May 15, 2020

against, the data subject will not be able to access the personal data processed by the device, they will not be able to correct any false information being processed (and which may lead to wrong inferences), and they will not have any rights surrounding automated individual decision-making, such as the right to obtain human intervention. They will also not have access to any of the legal recourse mechanisms provided for within the framework of the GDPR.

Moreover, this gap in the law exists only where the device is used by an individual for their own personal or household purposes. Where an enterprise uses the device, all rights of the GDPR are triggered to the benefit of the natural person using it – the enterprise would step into the role of responsible entity. As explained in an example given by the German Data Protection Supervisory Authorities in their 2019 'Report on Experience Gained in the Implementation of the GDPR':

> Locking systems are now available for front doors which do without a physical key. Users identify themselves using an app on their smartphone. Data are exchanged between the app and the producer (which is located in a third country with no adequate level of data protection).
>
> a) Where an enterprise uses such systems, the enterprise itself is the controller and thus responsible for data processing into which it has no insight. The producer is not a tangible presence in such contexts.
>
> b) Where natural persons use these systems in the course of a purely personal or household activity, there is no controller within the meaning of the GDPR. No-one is responsible under the GDPR, and the duties laid down in the Regulation come to nothing.
>
> Privacy and data protection would benefit greatly if the importer or trader, for instance, could be held accountable.[42]

It is hard to justify that the protections afforded to data subjects depend on factors such as the processing being used by an enterprise – or whether the data is processed locally on-device or remotely. The dangers for the data subject remain the same, i.e. being deprived of the GDPR's protections.

A challenge facing the approach of incorporating smart device manufacturers under the definition of controllers is where to draw the line between a smart (enough) device and a dumb device.[43] It is likely that not every AI, in the broad sense of the term, will be sufficiently developed to warrant a determination of the means and purposes of the processing by the producer. Drawing this line, however, is beyond the scope of this paper.

3. Conclusion

A fundamental shift has occurred in the way healthcare is delivered, bringing healthcare technology into patients' homes. The migration from the cloud to local processing in embedded

---

[42] Independent German Federal and State Data Protection Supervisory Authorities (*Datenschutzkommission*), 'Report on Experience Gained in the Implementation of the GDPR' (November 2019) 15. It appears that the report intended to include as a problem the issue of enforcing the GDPR in a third country such as China, arguably the country where most IoT devices today are produced. But the call to include either importers or traders is analogous to the call to include producers. For example, Section 4 of the German Act on Liability for Defective Products deals with the issue by defining a producer as also anyone who imports a product into the European Economic Area, and even the supplier of a product in those cases where the producer cannot be identified. German Act on Liability for Defective Products in the version promulgated on 12 December 1989 (Federal Law Gazette [*Bundesgesetzblatt*] I page 2198), last amended 17 July 2017 (Federal Law Gazette I page 2421).

[43] Unless the distinction between dumb and smart devices were to be dropped and *all* device manufacturers were classified as controllers to the extent that their products are directly offered to data subjects.
While we would appreciate the inclusion of all device producers under the GDPR, at least when it comes to the obligations of data protection by design and by default, it does seem somewhat of a stretch to extend the scope of controllership to producers of dumb devices against the clear indication of Recital 78 GDPR.

AI medical devices bring along new types of challenges and the web of actors involved has become increasingly more complex. This situation has exacerbated the boundaries for assessing data protection responsibilities even further. The responsibilities fall on data controllers and data processors, with controllers taking the heavier load. However, the current understanding of the controller/processor framework is too narrow in scope and in particular excludes producers of devices.

Our analysis of the various data processing scenarios depicted in this piece leads to the conclusion that the household exemption does not exempt all processing from the GDPR's scope; it only exempts local processing by the data subject. This also leads us to conclude that the prevailing distinction between local and remote processing is inadequate to distinguish whether processing is covered by the GDPR. The risks for the data subject remain the same, i.e., being deprived of the GDPR's protections. In addition, since end-users are not in the position to negotiate the terms of service or the functionality of AI medical devices, the concepts of 'joint' and 'sole' controllers, as possibly applicable following the CJEU's overly broad interpretation, may have reached their functional limits while nevertheless being too narrow in categorically excluding producers.

The inequality of bargaining power between device manufacturers and users creates an imbalance to the detriment of the latter. While most modern services grant users some degree of 'control' over the processing, this 'control' should rather be seen as a feature of the service itself and not as proper control in the meaning of the concept of 'controllership' under the GDPR. In our view, it is systematically and teleologically wrong to disrupt the assignment of roles between data subjects, controllers and processors, and assign the data subject responsibility for the processing. This is perhaps best evidenced when this responsibility would include the (possibly one-sided) obligation of entering into joint controllership and data processing agreements.

From our legal dogmatic analysis and teleological interpretation of EU court decisions, we argue that we need to re-examine the understanding of 'controllership' in such a way that takes into account the influence producers of embedded AI devices have. In particular against the backdrop of bringing healthcare services from hospitals to homes will require more than the mere production of AI medical devices, apps and services. It will also require designing and engineering technology that makes the most of this new setting while also respecting patient's autonomy, security and privacy.

Acknowledgement: This research is supported by a Novo Nordisk Foundation grant for a scientifically independent Collaborative Research Program in Biomedical Innovation Law (grant agreement number NNF17SA0027784). The opinions expressed are the authors' own and not of their respective affiliations.

Bibliography

Anderson R, Moore T, 'The Economics of Information Security', 314 *Sci* 610 (2006)

Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010)

Baumgartner U, 'Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen' in Eugen Ehmann, Martin Selmayr (eds), *Datenschutz-Grundverordnung* (C.H.Beck 2017)

Bird J, 'Artificial intelligence paves the way for fully automated diabetes kit' *Financial Times* (March 10 2020) <https://www.ft.com/content/15f0123e-3b7d-11ea-b84f-a62c46f39bc2> accessed May 15 2020

Bygrave L, ‘Article 25. Data protection by design and by default’ in Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler (eds), *The General Data Protection Regulation (GDPR) – A Commentary* (Oxford University Press 2020)

Castaldo S, *Trust in market relationships* (Edward Elgar Publishing 2017)

European Data Protection Board, ‘Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications’, version 1.0 (adopted on 28 January 2020)

Fennelly N, ‘Legal Interpretation at the European Court of Justice’ 20(3) *Fordham International Law Journal* [1996] 656

Forti, S., Ferrari, G-L, Brogi, A., (January 2020). ‘Secure Cloud-Edge Deployments, with Trust’ *Future Generation Computer Systems*. 102: 775–788; Buyya, R., Sriram, S., (eds) ‘Fog and Edge Computing: Principles and Paradigms’, Wiley Series on Parallel and Distributed Computing (John Wiley & Sons, 2019)

Hartung J, ‘Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen’ in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung/BDSG – Kommentar* (C.H.Beck 2018, 2nd ed)

Hartung J, ‘Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen’ in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung/BDSG – Kommentar* (C.H.Beck 2018, 2nd ed)

Independent German Federal and State Data Protection Supervisory Authorities (*Datenschutzkommission*), ‘Report on Experience Gained in the Implementation of the GDPR’ (November 2019)

Marcus G ‘Innateness, AlphaZero, and Artificial Intelligence’ *arXiv:1801.05667* (17 January 2018)

Metz C, ‘In Two Moves, AlphaGo and Lee Sedol Redefined the Future’ *Wired* (16 March 2016) <www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/> accessed May 15, 2020

Norwegian Consumer Council (*Forbrukarrådet*), ‘Out of Control’ (14 January 2020) <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/> accessed May 15, 2020

Office of the Australian Information Commissioner, 'Notifiable Data Breaches scheme 12-month insights report' (13 May 2019) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/> accessed 15 May 2020

Porumb, M., Stranges, S., Pescapè, A. et al., ‘Precision Medicine and Artificial Intelligence: A Pilot Study on Deep Learning for Hypoglycemic Events Detection based on ECG’ *Sci Rep* 10, 170 (13 January 2020)

Schneier B, ‘Economics and Information Security’ *Schneier on Security* (29 June 2006) <https://www.schneier.com/blog/archives/2006/06/economics_and_i_1.html> accessed 15 May 2020

Silver D et al, ‘Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm’ *arXiv:1712.01815* (5 December 2017)

Vinocur N, ‘One country blocks the world on data privacy’ *Politico* (25 April 2019) <www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/> accessed 15 May 2020