Cybersecurity Law Report
An Acuris company

cslawreport.com

June 17, 2020

GDPR

# The (Im)Possibilities of Scientific Research Under the GDPR

By Alex van der Wolk, *Morrison & Foerster*

Today, everything is about innovation. Many companies place an ever-strong emphasis on R&D as well as product and AI development using data analytics. While availability of underlying data for research purposes may not necessarily be an issue, use limitations typically apply where datasets consist of, or comprise, personal information. Companies often find themselves in a foothold where obtaining consent is impracticable (or even invalid), but using anonymous data may diminish the potential of the initiative. In this article, I will review the (im)possibilities of R&D under the GDPR. When does an activity qualify as "scientific research"? What requirements and constraints exist under the GDPR's "research exception"? How can you operationalize R&D activities so they still fit with the GDPR?

See also "Can GDPR Hinder AI Made in Europe?" (Jul. 10, 2019).

## Innovation Using Data

If there is one thing that companies have embraced in the last decade, it is the value and potential of data. You don't have to be Google to possess sizable databases, and chances are someone in your organization has already inquired or at least thought about whether that data can be used.

As companies look into the potential embedded in data, various forms of research come into play. For example, a vendor of a connected device probably wants to analyze how its customers use its device so it can improve the product. When is a device most often used? How does the customer configure the device? Under what circumstances does the device break down? Product improvement is a classic example of the use of data in a research context.

Research is not just limited to customer-facing parts of the business. The HR department may be very interested in analyzing data to get a grip on employees' attrition rate, with a view of retaining high-potential employees and generally bringing down the rate of employee turnover.

All of these examples involve the use of data for research purposes. And in all of these examples, the data at play contains personal information of individuals. Where any such use has a nexus to the E.U., the GDPR will have to be taken into account.

See also "Irish DPC Helen Dixon on GDPR Enforcement Hurdles One Year In" (May 29, 2019).

# The GDPR Framework

In order to be able to use any kind of personal information, the GDPR requires companies to have a "legal basis." Depending on the nature of the research, companies will generally assess whether they can rely on either consent, execution of contract or legitimate interest.

## Consent and Execution of Contract Often Not Practical

Whereas companies may quickly turn toward the individual's consent, this legal basis is often not practical or viable in a research context. For example, if you are running a clinical trial for research, you will want to ensure continued use of personal information. An individual's withdrawal of consent midway through a trial would be disruptive. Moreover, in an employee context, consent is generally considered invalid due to the subordinate relationship between employer and employee. Thus, companies may be keen on examining whether research initiatives can be undertaken on other legal bases than consent.

Execution of contract will also often not be a practicable option, as this basis is limited to where the processing of personal information is necessary to fulfill contractual obligations. It therefore requires an underlying contract between the individual and the organization that allows the company to engage in and perform research. Few research initiatives will be structured in this manner. In many cases, product development will be ancillary to service delivery, which according to E.U. guidelines means that execution of contract cannot be used to legitimize the development.

## Legitimate Interest

When consent or execution of contract cannot be used, companies will, in many cases, want to base their research on their legitimate interest. In its 2014 Opinion on Legitimate Interests, the Article 29 Working Party (a consortium of E.U. privacy regulators, under the GDPR renamed the "European Data Protection Board" (EDPB)) indicated that "processing for research purposes (including marketing research)" can, in principle, constitute a company's legitimate interest. However, in order for a company to be able to rely on its legitimate interest, it must evaluate the interests of the company against the impact of the processing on the privacy rights of the individual. Essentially, the legitimate interest test requires a weighing of the "pros and cons."

For example, if the results of the research not only benefit the company, but also the individual, or have more broad societal benefits (*e.g.*, according to recital 257 of the GDPR: knowledge about "widespread medical conditions" and the "long-term correlation of a number of social conditions"), the research may very well be undertaken on the basis of legitimate interest. If, however, it is only the company standing to benefit, it is unlikely that legitimate interest is the appropriate legal basis.

## Sensitive Personal Information

Where "sensitive" personal information is at stake, additional restrictions apply. Sensitive personal information includes health and medical information, political opinions, racial or ethnic origin, and sexual preference. Under the GDPR, it is prohibited to process sensitive personal information unless an exception

applies. And while "explicit consent" provides for such exception, here too, the impracticalities around consent (as previously discussed) are present. As such, companies engaging in research using sensitive personal information will, in many cases, want to try to benefit from the "research exception."

# The Research Exception Further Examined

Article 9(2)(j) of the GDPR provides for the possibility of processing sensitive personal information where "processing is necessary for scientific or historical research purposes or statistical purposes," provided the processing is undertaken "in accordance with Article 89()1) GDPR" and is "based on Union or Member State Law." This means that the research exception comes with a host of conditions.

## When Does Research Qualify as "Scientific Research"?

While "research" is not explicitly defined in the GDPR, there are indications it should still be understood to be a broad notion. Recital 159 to the GDPR provides that scientific research can be undertaken by both public and private entities, as is evidenced through the examples of scientific research: technological development and demonstration, fundamental research, applied research and privately funded research, as well as public health research. Recital 54 provides that public health includes "all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, healthcare needs, resources allocated to healthcare, the provision of, and universal access to, healthcare as well as healthcare expenditure and financing, and the causes of mortality."

However, it still leaves open the question whether any and all research by a company (including, for example, product development) would fall within the research exception. The GDPR does not explicitly answer that question, although recital 159 does provide that "specific conditions should apply in particular as regards the publication or otherwise disclosure of personal information in the context of scientific research purposes." The recital also cites Article 179(1) of the Treaty on the Functioning of the European Union, which promotes "the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely."

At a minimum, this suggests that there needs to be some form of public or external component to a company's scientific research (regarding the research insights and results – not any underlying personal information). The argument that consumers will be able to benefit from better products will likely not satisfy the public component. At the same time, it also remains open how much of the research should be made publicly available, for example, whether just the research outcomes and insights would suffice or whether underlying raw research results also should be published.

## "Appropriate Safeguards"

In order for a company to benefit from the research exception for sensitive personal information, article 89(1) of the GDPR needs to be observed. This article requires that a company that uses the research exception implements "appropriate safeguards," which entails implementing "technical and organizational measures" to ensure that only the personal information necessary for the research purposes are used (*i.e.*, applying the principle of data minimization).

One way for a company to comply with this requirement is by applying pseudonymization. Pseudonymization (also referred to as key-coding or hashing) is the processing of personal information in such a way that the information can no longer be attributed to a specific individual without the use of additional information. With this additional information, pseudonymized data can technically be re-identified.

Pseudonymization entails keeping the key or hash used to re-identify separate and secure to prevent re-identification from being undertaken within the research itself. Pseudonymization is not always required, but rather its use is encouraged if the research purposes can be fulfilled using pseudonymized data. The GDPR also notes that, where the research purposes can be fulfilled using anonymous data, such anonymous data should be used. The issue of anonymization is revisited below.

## Union or Member State Law

In order for the research exception to apply, the possibility for scientific research using sensitive personal information needs to also be embedded in Member State law. In other words, the GDPR itself only provides for the general framework, but the actual possibility for relying on the exception needs to be provided for in national law. Such national laws may provide for further requirements.

Indeed, there are many national law requirements that go well beyond the GDPR. For example, in Italy, the research may not lead to measures or decisions with respect to a particular individual, and in the U.K., the individual may not experience substantial damage or distress from the research.

In the Netherlands, in order to benefit from the research exception, it must be evidenced that it is impossible or requires disproportionate effort to obtain the individual's explicit consent. Thus, the Dutch GDPR Implementation Act suggests that scientific research should first and foremost be undertaken on the basis of explicit consent (not the research exception) and, only if that is not possible, on the basis of the research exception. Furthermore, where the research exception is used, the research has to serve a public purpose and there may not be any undue impact on the individual's privacy.

In Ireland, companies wanting to benefit from the research exception must (amongst other things) implement an appropriate governance structure (which includes obtaining ethical approval by an ethical research committee), create an audit trail, *and* obtain explicit consent from individuals taking part in the research. Companies can forego explicit consent only if they obtain a declaration from a Committee appointed by the Ministry of Health, which will evaluate whether there is a strong enough public health component to the research. By making "explicit consent" a sub-requirement of the research exception, it makes one wonder why companies would not rely on the exception of explicit consent in the first place, without all the additional requirements under the research exception.

Suffice it to say that the further national implementation of the research exception is far from uniform, and companies will therefore unfortunately have to assess additional requirements on a country-by-country basis.

See also the CSLR's three-part series analyzing early GDPR enforcement: "Portugal and Germany" (Jan. 23, 2019); "U.K. and Austria" (Jan. 30, 2019), "France" (Feb. 6, 2019).

## The Challenges of Anonymization

Another possibility for legitimizing research (for both "regular" and "sensitive" personal information) is to anonymize the data such that the GDPR no longer applies. However, E.U. privacy regulators set high requirements on anonymization. They approach anonymization almost statistically, considering the theoretical possibility of re-identification of a dataset post-anonymization. In order for personal information to be "truly" anonymized, there should be a near-zero-percent chance of re-identification. And while anonymization techniques become better and better, so do re-identification techniques. Creating a sufficiently anonymized data set comprising of personal information is often very challenging. As a result, E.U. privacy regulators often consider anonymized datasets to still be subject to the GDPR and review the degree of anonymization as a security measure more so than a measure that will take the dataset out of GDPR applicability.

Companies that want to use anonymization so that they can use personal information in their research will have to go to great lengths to make this happen. Moreover, companies should keep a close eye on the maintained usability of an anonymized dataset, which can quickly decrease when the level of anonymity increases.

See also our three-part series on GDPR essentials for the financial sector: "Benchmarking and Assessing the Risks" (Jul. 11, 2018); "Compliance Steps" (Jul. 18, 2018); and "Staying Compliant and Special Challenges" (Jul. 25, 2018).

## The Challenges of Purpose Limitation

Another challenge under the GDPR is that personal information may only be used for specified and explicit purposes. At the time of collecting personal information, a company must have determined and specified for which specific purpose(s) the information will be used. This means that if personal information is first obtained for research purposes, the nature and scope of the research will have to be specified. "Research purposes" generally will not be sufficiently specific. This puts limitations on the ability to use personal information obtained for one specific research project for another (even if the information was obtained with the explicit consent from the individual). It also requires companies to already have a clear view on the nature and objectives of a research project before commencing. This makes it challenging to undertake projects where the purpose of the analytics is to identify and formulate the scope of the actual subsequent research.

Similar challenges exist with personal information that was originally obtained for purposes other than research altogether. For example, HR data, warranty data, access and use logs, etc., all are typically compiled and collected for other purposes than just research. The GDPR provides that personal information can be used for purposes other than for which the information was originally obtained, but only if such "secondary purposes" are not incompatible with the original purpose. The compatibility test requires companies to assess how closely the original and secondary purpose are related, but also to consider the nature of the personal information and the reasonable expectations of

the individual. The more remote the original purpose is from the research objectives, the more likely such purposes will be incompatible. This is particularly true for companies that obtain personal information in a service provider role. Where personal information is obtained as part of a service contract (*e.g.*, maintenance and support, hosting, or remote servicing), contracts with the customer will often provide that such information can only be processed on behalf of the customer (*i.e.*, in a processor role). In such case, the service provider will not be able to simply reuse the information for its own (research) purposes.

## The Way Forward

It will be clear that companies that want to engage in research initiatives in the E.U. will need to work their way through a myriad of assessments and requirements. The inability of the GDPR to provide for a clear and workable way forward for companies undertaking research projects does not seem to be on par with the E.U.'s objectives of fostering innovation as part of the E.U.'s Digital Single Market strategy. The varying degree of requirements at a national level combined with the strong requirements toward (explicit) consent, pseudonymization, and anonymization make it challenging for companies to navigate their research projects into GDPR compliance whilst making full use of their research potential. The result may well be that companies will be drawn to countries outside the E.U. where their projects do not face similar restrictions.

*Alex van der Wolk is the co-chair of Morrison & Foerster's global privacy and data security practice. Based in Brussels and London, he advises global companies on their most complex data protection strategy and compliance governing all aspects of information management. Van der Wolk helps clients develop privacy strategies for digital transformations, industrial IoT, telematics, big data, commercial and marketing programs and data analytics.*