BIO DEUTSCHLAND
Biotechnologie-Industrie-Organisation Deutschland e. V.

Position of BIO Deutschland

Topic: Comments on the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) of the European Data Protection Board

Introduction

BIO Deutschland thanks for the opportunity to comment on the European Data Protection Board`s "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)". Especially the issue of the representative of the controller or processor has some impact on the conduct of clinical trials in the European Union by non-EU sponsors. To keep the EU attractive as a region for non-EU sponsors to conduct clinical trials, the guideline text should be more detailed and in closer compliance with the GDPR for the following topics:

1. Exemptions from the obligation to designate a representative - section 4 b)

The guideline of the European Data Protection Board (EDPB) on the exemptions from the obligation to designate a representative do not help controllers or processors to determine whether their activities qualify for the exemption of article 27 (2) General Data Protection Regulation (GDPR), when they do "not include, on a large scale, processing of special categories of data as referred to in Article 9 (1)".

> ***Guidelines 3/2018 states**: While the GDPR does not define what constitutes large-scale processing, the WP29 has previously recommended in its guidelines WP243 on data protection officers (DPOs) that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale: the number of data subjects concerned - either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity.*

The guidelines of the EDPB are much too vague and only provide ideas to supervisory authorities to invent their own criteria. The EDPB should define clear and transparent guidelines, ideally definite ones, with real numbers and explicit conditions. This includes answers to the following questions:

If only one piece of a special category of data per data subject is collected (e.g. infection with influenza virus: yes or no), what is upper limit of data subjects before the data processing becomes large scale?

In this example, what would be the upper limit of proportion before this processing becomes large scale?

What is the population of data subjects for which the proportion is calculated (is it the population of the whole EU, the population in one member state, the population of elderly in one member state?)? Suppose that N is the upper limit of the data subjects in this example. Would the processing become large scale if the data subjects were not only in one EU member state but in two? Or would processing become large scale if the data subjects were from three or four EU member states?

What would be the limiting number of EU member states before "the geographical extent of the processing activity" in this example would make the data processing large scale?

Suppose that only one piece of a special category of data from 100 data subjects is processed, but in all 27 EU member states. Would this qualify as large scale processing? If yes: What would be the limit of numbers of EU member states before the "the geographical extent of the processing activity" becomes large scale?

Suppose that in the initial example the data are processed for one month and that this would still be below large scale. What is the limit for processing time that would turn it into large scale?

The EDPB might resort to the position that exact criteria for large scale have to be determined on a case by case basis, but this position makes determinations of the supervisory authorities totally arbitrary and unpredictable. Since the definition of large scale determines compliance with the rules of GDPR for assignment of a representative, unpredictable and random ad hoc criteria are unacceptable.

2. Representatives in clinical trials – section 4 c)

The example the EDPB describes for clinical trials does not describe the setting for clinical trials in a realistic way.

> ***Guidelines 3/2018 states***: *Example 20: An Indian pharmaceutical company, with neither business presence nor establishment in the Union and subject to the GDPR as per Article 3(2), sponsors clinical trials carried out by investigators (hospitals) in Belgium, Luxembourg and the Netherlands. The majority of patients participating to the clinical trials are situated in Belgium.*
>
> *The Indian pharmaceutical company, as a data controller, shall designate a representative in the Union established in one of the three Member States where patients, as data subjects, are participating to the clinical trial (Belgium, Luxembourg or the Netherlands). Since most patients are Belgian residents, it is recommended that the representative is established in Belgium. Should this be the case, the representative in Belgium should however be easily accessible to data subjects and supervisory authorities in the Netherlands and Luxembourg.*
>
> *In this specific case, the representative in the Union could be the legal representative of the sponsor in the Union, as per Article 74 of Regulation (EU) 536/2014 on clinical trials, provided it is established in one of the three Member States, and that both functions are governed by and exercised in compliance with each legal framework.*

In reality, the Indian pharmaceutical company would not only conduct one clinical trial at a time but several of them, which follow one another during the development of a medicinal product. This could take a whole decade or more. When starting the first trial in the EU it is hard to determine where the majority of patients will be situated which the Indian company will enroll in the set of trials for the whole development program. The first phase I trial in the development of a medicinal product might be conducted only in Belgium, but a subsequent phase II trial might be conducted in France, a phase III trial many years later might be conducted in Germany, Italy, Spain, etc. Given that, should the Indian company move the representative from Belgium to France and then then to Germany? Should the company monitor on an annual basis where the majority of the patients is? This might involve to check which patients died after the end of the trial, which necessitates the collection of more data than the controller would usually collect. It is impossible to predict at the beginning were later trials will be conducted and where the majority of patients will be enrolled. When the representative is moved to the country with the new majority of patients in phase II trials, do patients of phase I have to be informed about that fact (according to article 14 (1) a GDPR)? If this has to be done, the controller would have to collect more data about the data subjects than it would normally do. This shows that the recommendation to place the representative in the country with most of the patients is not advisable.

It is also questionable whether the sponsor's legal representative could and should assume the role of the data controller's representative. First, one sponsor can assign separate legal representatives for each of the trials which are active in parallel or subsequently. However, the controller can assign only one representative at a time (or can more be assigned?) and it might be best practice that this one remains constant for a long period, because switching from one (data controller) representative to another too often will necessitate, in the context of clinical trials, that patients of already finished trials would have to be informed about these switches as long as their personal data are processed. As Regulation (EU) 536/2014 demands storage times of at least 25 years, and as according to article 4 (2) GDPR, "storage" is processing of data, personal data from a trial will have to be processed decades after the trial has ended. This does no ban an entity which was the sponsor's legal representative only in a phase I trial to serve as a controller's representative from

phase I to phase III trials, but it could be questioned whether this is or should be a common approach or even best practice.

Second, the scope of representation and review activities of the sponsor`s legal representative and the controller`s representative are quite different. A sponsor's legal representative is responsible often for only one, sometimes for more clinical trials of one sponsor company. The sponsor company, as a controller, might conduct data processing activities in the EU that have nothing to do with the clinical trial. E.g. the controller might collect data from sales representatives, from consultants, from medical doctors visited by sales representatives, from consumers of marketed medicinal products etc. The sponsor's legal representative is not in good position to monitor these activities (if the EDPB expects that data protection representatives monitor something at all).

The third problem with this issue is: The EDPB argues in this Guideline 3/2018 that it "does not consider the function of representative in the Union as compatible with the role of an external data protection officer" as the data protection officer should have a considerable degree of independence which the controller's representative does not have. The question is whether the sponsor's legal representative according to article 74 of Regulation (EU) 536/2014 would not partly be in a similar role as the external data protection officer. According to article 74 (1) of Regulation (EU) 536/2014 the "legal representative shall be responsible for ensuring compliance with the sponsor's obligations". This task might necessitate some independence and it echoes some of the tasks of the data protection officer as defined in article 39 GDPR. The issue of the exact role of the sponsor's representative is still not settled and before there is legal certainty EDPB should not recommend that sponsor's legal representatives could assume the role of a controller's representative. **We propose the following wording**:

> *Example 20: An Indian pharmaceutical company, with neither business presence nor establishment in the Union and subject to the GDPR as per Article 3(2), sponsors clinical trials carried out by investigators (hospitals) in several EU member states. The clinical trials are conducted over a period of 15 years and cover phases I to III. Belgium, Luxembourg and the Netherlands*
>
> *The Indian pharmaceutical company, as a data controller, shall designate a representative in the Union established in one of the Member States where patients, as data subjects, are participating to the clinical trial. It is hard to predict where most patients will be recruited, therefore it is not possible to make sure that the representative is stablished in that EU member state where the majority of patients will be recruited.*
>
> *If the first phase I trial is conducted in Belgium, and none of the following trials is conducted in this country, the representative of the Indian pharmaceutical company could still be located in Belgium during a phase III trial, 10 years after the end of the phase I trial, as long as personal data of the phase I trial are stored or otherwise processed.*
>
> *It might be possible but it is not recommended that in this specific case, the representative in the Union should be the legal representative of the sponsor in the Union, as per Article 74 of Regulation (EU) 536/2014 on clinical trials. One reason is that the sponsor might assign different representatives for each of the trials while there should only be one controller representative. A second reason is that the scope of responsibility of a sponsor's legal representative and a controller`s representative are different: A controller`s representative represents the controller in much more data procession activities than those involves in a clinical trial. Another reason is that the sponsor's legal representative might need more independence from the sponsor, according to Article 74 of Regulation (EU) 536/2014, than the GDPR allows for the controller's representative.*

3. Language capabilities of the representative - section 4 d)

The GDPR has no provisions for the language capabilities of the representative, not even for the language capabilities of the controller. The GDPR implicitly allows that communication takes place in any language.

Guidelines 3/2018 states: With the help of a team if necessary, the representative in the Union must therefore be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a representative is therefore essential in order to ensure that data subjects and supervisory authorities will be able to establish contact easily with the non-EU controller or processor.

> ***Guidelines 3/2018 states**: With the help of a team if necessary, the representative in the Union must therefore be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a representative is therefore essential in order to ensure that data subjects and supervisory authorities will be able to establish contact easily with the non-EU controller or processor.*

It cannot be expected that a representative has the capability to communicate in all languages of the EU and beyond: As the GDPR applies not only to EU citizens but to all "Data subjects who are in the Union" (Article 3 (2) GDPR), data subjects could speak all languages of the planet earth. It cannot be expected that the representative is able to provide language experts for all of these languages. As GDPR does not set clear demand for languages necessary EDPB should not generate unnecessary burden. A clear statement for an efficient communication is strongly recommended.

The GDPR does not implement the representative primarily as a contact point for data subjects but as a contact point for supervisory authorities (see recital 80 GDPR). The fact that the data subjects should be informed about the identity and contact details of the representative (according to articles 13 and 14 GDPR) does not inevitably imply that the representative has to speak the language of any data subject. It should be enough that the representative can ensure effective communication.

The fact that data subjects are informed that they have the right to lodge a complaint with a supervisory authority (according to articles 13 and 14 GDPR) does not mean that e.g. the supervisory authority of a controller in Slovakia has to have the capability to communicate with Turkish speaking data subjects in Germany. **We propose the following wording:**

> *GDPR has no provisions about the language capacities of the representative. To enable communication the representative should have the capacity to communicate with the supervisory authorities and data subjects, preferably in English. It is advisable that the representative takes care of capacities to communicate in the languages of the EU member states where the data subjects are located whose data are processed, but this is not a legal requirement.*

4. Liability, administrative fines and penalties imposed to the representative - section 4 d)

The GDPR does not specify liability of the representative or which administrative fines and penalties should be imposed. While the Guidelines 3/2018 should shed some light on these issues, it remains silent. Therefore we ask the EDPB to provide guidance, taking into account the following issues:

> ***Guidelines 3/2018 states**: It should however be noted that the concept of the representative was introduced precisely with the aim of ensuring enforcement of the GDPR against controllers or processors that fall under Article 3(2) of the GDPR. To this end, it was the intention to enable enforcers to initiate enforcement action against a representative in the same way as against controllers or processors. This includes the possibility to impose administrative fines and penalties, and to hold representatives liable.*
>
> ***Recital 80 GDPR states**: The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation.*

It has to be clarified which liability remains with the representative and what the representative could do to remain not liable. As a part of this, the EDPB has to define the representative's obligations and responsibilities.

> ***In section 4 d) the Guideline 3/2018 states****: As clarified by recital 80, the representative should also perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. In practice, this means that a supervisory authority would contact the representative in connection with any matter relating to the compliance obligations of a controller or processor established outside the Union, and the representative shall be able to facilitate any informational or procedural exchange between a requesting supervisory authority and a controller or processor established outside the Union.*

There are two angels in this paragraph. On the one hand the representative can only act in the range of the mandate given by the controller or processor. A liability is therefore only possible for actions/obligations which lay in the hand of the representative and not in the hand of the controller or processor. On the other hand recital 80 and Article 27 (5) GDPR clearly state that the appointment of a representative does not affect the liability and accountability of the controller or processor. However, if the representative is liable (especially for actions taken by controller or processor), the controller or processor will be exonerated at the same time and these regulations will be undermined.

Article 3 (1) and (2) in conjunction with Article 27 GDPR provide a graduated relationship (see last paragraph on 4. of Guideline 3/2018). The appointment of a representative in the EU does not mean that a controller or processor in the EU are present (according to Art. 3 para. 1 GDPR). Rather, a representative regulation is made via Art. 27 GDPR. Unfortunately, Art. 27 does not clarify the liability of the representative. However, Article 27 (4) and (5) GDPR clearly states that the representative (in addition to the controller or the processor) is the local point of contact for the supervisory authorities and data subjects (paragraph 4) and the designation does not prejudice legal action against the controller or processor (paragraph 5).

A possible approach for the representative to avoid liability could be the review of data processing activities of the controller or processor and the request for corrective actions, if the representative finds non-compliance with GDPR. In most cases this will be out of the scope of the mandate. A review of activities out of the scope could lead to court actions between controller or processor and representative because of the breach of the written mandate. Therefore EPDB should clarify the liability of the representative. The GDPR does not attribute any reviewing activity to the representative. Does the EDPB regard this reviewing activity to be compliant with the concepts of the GDPR? The EDPB states in Guidelines 3/2018 that it “does not consider the function of representative in the Union as compatible with the role of an external data protection officer” because the representative lacks a sufficient degree of autonomy that the data protection officer needs. If the representative is expected to review the data processing activities of the controller and is expected to advise the controller to change its processes, the representative would need a degree of autonomy that the EDPB believes is missing. Probably for very good reason: If the representative would start to act against the mandate of the controller, it would effectively become a controller itself. This is probably not intended by the GDPR.

However, if the representative has no means to purge itself from liability, it is doomed to be a blind and paralyzed letterbox with an inbuilt cash machine for paying penalties. It could only get active against the mandate if the processor or controller when switched on by the supervisory authority. It is questionable whether this is an attractive job and whether the GDPR actually intends to establish such a job description. The EDPB should explain whether it believes that a representative should act like that.

A way of interpretation of the GDPR`s concept of the representative that appears to cause the minimum of incoherence with the provisions of the GDPR is that the representative is actually not much more than a letterbox without liability. This interpretation might be unsatisfactory, but it appears to be more plausible than other concepts. In fact, articles 83 and 84 GDPR do not list any administrative fines or penalties specific for representatives, it only lists fines and penalties controllers and processors. During the legislative process, the Council of the European Union inserted an Article 79 (3a) GDPR, which read: “Where a representative has been designated by a controller pursuant to Article 25, the administrative fine may be imposed on the representative without prejudice to any proceedings which may be taken against the controller” (see: Council of the European Union, document No 11013/13). However, this provision was deleted in the further discussion of the GDPR by purpose, meaning that there is no more legal basis for administrative fines imposed on the representative. Even if it was correct “that the concept of the representative was introduced precisely with the aim of ensuring enforcement of the GDPR against controllers or processors […] [and] it was the intention to enable enforcers to initiate enforcement action against a representative in the same way

as against controllers or processors" this intention itself does not constitute a norm if it is not materialised as a norm. The fact is that the intention is not materialised as a norm and the EDPB is not empowered to establish norms.[1] **We propose the following wording**:

It should however be noted that the concept of the representative was introduced with the aim of ensuring enforcement of the GDPR against controllers or processors that fall under Article 3(2) of the GDPR. However, even if the representative is addressed by enforcement actions, the representative can react only according to a mandate by the controller or processor it represents. This means that the controller or processor are expected to advise the representative in which way to react to the enforcement actions. Once the representative reacts without mandate, it essentially becomes a controller itself. The GDPR does not empower supervisory authorities to enforce representatives to become controllers. The GDPR has no provisions to impose administrative fines and penalties on the representative. As long as the representative acts according to its mandate, it cannot be held liable. In this case only the controllers or processors are liable.

[1] see also, L Franck. RDV 2018(6): 303ff.; Schlender, in Gierschmann, Schlender, Stentzel, Veil: Kommentar Datenschutz-Grundverordnung, § 27, Note 21)

BIO DEUTSCHLAND
Biotechnologie-Industrie-Organisation Deutschland e. V.

This position paper was made by the Regulatory Affairs Working Group of BIO Deutschland

As the sector association of the biotechnology industry, Biotechnologie-Industrie-Organisation Deutschland e. V. (BIO Deutschland) with its more than 320 members, has set itself the objective of supporting and promoting the development of an innovative economic sector based on modern biosciences. Dr. Peter Heinrich is head of the board of BIO Deutschland.

Supporting members and industry partners of BIO Deutschland are Abbvie, Avia, Bayer Pharma, Boehringer Ingelheim Pharma, Clariant Produkte (Deutschland), CMS Hasche Sigle, Deutsche Bank, EBD Group, EY, Isenbruck │ Bösl │ Hörschler, Janssen, KPMG, Merck, MiltenyiBiotec, MorphoSys, PricewaterhouseCoopers, Qiagen, Roche Diagnostics, Sanofi-Aventis Deutschland, SAP, Thermo Fischer, Vertex und VWR.

Contact

Further information of the work of BIO Deutschland are available on www.biodeutschland.org.

BIO Deutschland e. V.
Schützenstraße 6a
10117 Berlin

Tel.: 030-23320164-30
Fax: 030-23320164-38
E-Mail: info@biodeutschland.org
web: www.biodeutschland.org