MORRISON | FOERSTER

250 WEST 55TH STREET
NEW YORK, NY 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

BEIJING, BERLIN, BRUSSELS,
DENVER, HONG KONG, LONDON,
LOS ANGELES, NEW YORK,
NORTHERN VIRGINIA, PALO ALTO,
SAN DIEGO, SAN FRANCISCO, SHANGHAI,
SINGAPORE, TOKYO, WASHINGTON, D.C.

January 23, 2018

Writer's Direct Contact
+1 (212) 506.7213
MWugmeister@mofo.com

Submission from the Global Privacy Alliance to the Article 29 Data Protection Working Party on Guidelines on Consent under Regulation 2016/679

The Global Privacy Alliance (GPA) welcomes the opportunity to comment on the Guidelines on Consent under Regulation 2016/679 ("Guidelines") issued by the Article 29 Working Party ("Working Party").

The GPA is comprised of a cross section of global businesses from the automobile, aerospace, communications, computer and computer software, consumer products, electronic commerce, financial services, logistics, pharmaceutical, medical devices, and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

Consent remains one of six lawful bases to process personal data under the GDPR but there are new requirements for obtaining and demonstrating valid consent. While the Guidelines provide important guidance on how to implement these new requirements, we have concerns in the following areas: granularity of consent, deletion of research results, the minimum content requirements for consent to be "informed", the need to specify upfront all purposes of processing, particularly with respect to research activities, and the requirement to match up each purpose and each data element with a specific legal basis.

I. Granularity

The Guidelines state that for services involving multiple processing operations for more than one purpose, individuals should be free to choose to which purposes they consent, rather than having to consent to a bundle of processing purposes. The Guidelines advise that several consents may be warranted in such situations.

This proposed approach to have multiple consents, which is similar to the consent approach in a few other countries, would mean that individuals will need to click multiple times with the practical effect that individuals will likely stop reading the notices and simply click multiple times. Notice and consent "fatigue" a problem recognized in the Guidelines, is a serious issue in this context. As an alternative, organizations should be able to offer a bundled consent for a particular product or service. For example, in the online gaming platform example (#17), individuals that subscribe to the service would need to consent to participate in an online game and consent that their information can be shared with other players of the game and sponsors who are providing the platform for free. This consent should not involve two separate consents. Rather individuals should be able to agree that their information will be collected by the game and shared with other players. In this context, the two consents go together. An individual cannot agree to share the information with the company and not with other players. Similarly, the individual cannot agree to share the information with other players and not with the company. So in order to participate in the online game, the player should be able to agree by clicking one click rather than two. This approach is consistent with Recital 32 which states that "the request [by electronic means] must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

In sum, if the purposes of processing are so inter-related that the individual does not truly have the ability to say yes to one and no to the other and still participate in the activity, then requesting two consents should not be required as it becomes meaningless and will simply result in consent fatigue.

II. Deletion of Research Results

The Guidelines also state that if a controller is relying on consent and the individual withdraws his/her consent, then the controller must delete or anonymize the personal data immediately if it wishes to continue to use the data for research purposes. However, deletion of scientific research results upon withdrawal is inconsistent with Good Clinical Practice as well as international and EU rules.[1]

[1] Recital 76 of the EU Clinical Trial Regulation (No 536/2104) states "With a view to respecting those rights, while safeguarding the robustness and reliability of data from clinical trials used for scientific purposes and the safety of subjects participating in clinical trials, it is appropriate to provide that, without prejudice to Directive 95/46/EC, **the withdrawal of informed consent should not affect the results of activities already carried out, such as the storage and use of data obtained on the basis of informed consent before withdrawal**." Article 28.3 also states "Without prejudice to Directive 95/46/EC, **the withdrawal of the informed consent shall not affect the activities already carried out and the use of data obtained based on informed consent before its withdrawal**."

Retention of patient data is essential to the conduct of a successful clinical study. Individuals may withdraw their consent to continue participation in the study because they are having an adverse reaction to the drug that is the subject of the trial. This is not the same as withdrawal of consent for processing or automatic deletion of data. If as a consequence of the withdrawal of consent, a clinical site were to delete the data relating to that individual, then all of the information regarding the adverse reaction to the drug would also be deleted. This would undercut the validity of clinical trials and be contrary to all of the Good Clinical Practices[2] that regulate clinical trials. If at the end of a clinical trial, a significant number of patients are missing outcome data, there may not be enough pool for data analyses to conclude a study based on its objectives. If the data of patients who are either lost to follow-up or who withdraw consent during the clinical study are eliminated from the data pool, this elimination subsequently and directly affects the validity of conclusions derived from the clinical study.

The need to retain the data already collected is essential to guarantee the integrity of the study and assess the quality of the study results. In fact, all of the relevant clinical and research guidelines that are in place in Europe require that the clinical site retain patient data when an individual withdraws from research. Thus the WP29 has set up a direct conflict of laws for scientific research organizations and the position taken in the draft guidelines needs to be aligned with the Good Clinical Practice obligations under EU law.

III. Minimum Content Requirements for Consent to be 'Informed'

The Guidelines state that where the data are to be transferred to or processed by other controllers who wish to rely on the original consent, these organizations should all be named in the notice. However, in some cases, it is not always possible to fully identify all recipients

---

The FDA Guidelines on withdrawal from FDA regulated clinical trials states that "(…) data collected on study subjects up to the time of withdrawal must remain in the trial database in order for the study to be scientifically valid. **If a subject withdraws from a study, removal of already collected data would undermine the scientific, and therefore the ethical, integrity of the research.** Such removal of data could also put enrolled subjects, future subjects, and eventual users of marketed products at an unreasonable risk. Finally, removal of data would fundamentally compromise FDA's ability to perform its mission, to protect public health and safety by ensuring the safety and effectiveness of regulated products."

[2] *See* Integrated Addendum To ICH E6(R1): Guideline For Good Clinical Practice, page 24 (which require that **"there is no deletion of entered data** (i.e., maintain an audit trail, data trail, edit trail").

and/or purposes. Recital 33 recognizes this reality in the context of scientific research. In the context of the Internet Of Things ("IoT") where there is an entire eco-system, naming all of the other controllers in the ecosystem will be virtually impossible. For example, if a consumer has elected to allows his refrigerator track when the family is out of milk and provide that information to the grocery store so that the milk can be delivered by a delivery company, it will be the consumer (not the company that provides the refrigerator) who will elect which grocery store and which delivery company will receive his data. The company that makes the refrigerator and provides the ability of the consumer to share information with other data controllers will not have control over or even know everyone with whom the consumer elects to share personal data. In the context of IoT and similar situations, requiring organizations to disclose the categories of controllers is much more consistent with the way in which these types of services will operate and more accurately reflects who is making decisions regarding the sharing of personal data.

IV. Specified Purposes

GDPR Articles 9.2 and 89(1) and Recitals 33, 50,159 and are intended to protect scientific research because it is a public interest to the EU. Many positive results are now being achieved by using existing scientific research to find new solutions to existing problems. Further, secondary research purposes that result from previously collected data are providing new insights and discoveries. Recital 33 of the GDPR specifically recognizes the need for a flexible approach when it comes to specifying the purposes of use and obtaining granular consent for scientific research because of the importance of scientific research to the public.

The Working Party Guidelines seems to send a contradictory message by restricting the scope of a valid consent for scientific research. The Working Party takes the position in the Guidelines that scientific research projects that fail to provide granular purposes and obtain consent on the basis of those stated purposes will have difficulty demonstrating compliance with GDPR requirements. In particular, where the research purposes are not fully specified from the outset and the research involves sensitive data, the controller must obtain new consents before commencing new stages of research.

The Working Party's proposed approach would make it very difficult if not impossible for companies to conduct scientific research aimed at summarizing a field of research, looking at a problem in a new way. For example, a significant period of time often elapses between when a specific scientific research project ends and when subsequent research begins. Thus patients may no longer be reachable as they may have changed addresses. Often research projects rely on data collected by the public health system, which would then require contacting the population of an entire country to seek consent, which of course would be impossible. Moreover, it is impossible to fully know how the data can be used for scientific breakthroughs during the initial consent period, because additional research may not be possible to plan until the knowledge is gained from the initial research.

These requirements would essentially make it impossible to do scientific research based on existing data or to do secondary research and are inconsistent with the data minimization principles. Given the importance of scientific research to the EU, the requirements with the data protection rules should not undermine that important public interest. Organizations engaged in scientific research should be able to seek consent from the participants in a study even if the contours of the subsequent research are not fully known, consistent with statements contained in Recital 33.

V. More than one Legal basis

The Guidelines state that: "In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis." This scenario does not recognize instances where the same personal data may be processed for multiple purposes, each of which may rely on different legal bases. Thus continued processing may not be an instance of swapping between one legal basis and another, but may be completely legitimate. For example, while an individual's name and email address may be used to market new products to the individual (on the basis of consent), this same information may be used to provide the services purchased by the individual (contractual necessity), and used for fraud prevention purposes (legitimate interests). Thus even if the individual withdrew consent for marketing, the organization could continue to process the personal information for the other legitimate purposes.

The Guidelines' proposed approach is inconsistent with Article 17(1)(b) of the GDPR Article which states that a controller must delete information when an individual withdraws consent "where there is no other legal ground for processing." That language strongly suggests that there can that processing may be carried out on the basis of consent as well as other legal grounds and that the controller can determine at the time of the withdrawal of consent whether there are other legal bases for processing.

Moreover, the Guidelines state that a notice must be sufficiently detailed – in particular, for each purpose a controller must specify "each element of data and which lawful basis is being relied upon". Such a requirement exceeds the requirements of the GDPR (Article 13(1)(c) and will be unworkable in practice. This requirement would mean that a notice would be dozens of pages long. If an organization has multiple purposes of processing, it would need to list each purpose, then each data element and then the legal basis. Providing this information would not in any way enhance the understanding of the individual and would simply make the notices unwieldy and inconsistent with the Working Party's stated goal of having short and understandable notices.

A more effective approach would be to clearly identify in the notice the processing activities that are being carried out on the basis of consent and the choices available to the individual with respect to cessation of processing and deletion of personal data. While the notice should also describe the other purposes of processing and the other legal grounds for such processing, consistent with Article 13(1)(c), there should be no requirement to match up each purpose and each data element with a specific legal basis.