36.

SIIA Accelerating Innovation in Technology, Data & Media

January 31, 2016

Ms. Isabelle Falque-Pierrotin
Chairman
Article 29 Data Protection Working Party
JUST-ARTICLE29WP-SEC@ec.europa.eu
presidenceg29@cnil.fr

Dear Madame Falque-Pierrotin:

I am writing to you and your colleagues on the Article 29 Working Party on behalf of the Software & Information Industry Association (SIIA), which is the principal trade association for the software and digital content industries worldwide. The association provides global services in government relations, business development, corporate education, and intellectual property protection to its members, the leading companies that are setting the pace for the digital age. SIIA is engaged in the European policy debate and has organized conferences and events on issues of interest to European policymakers in Brussels, London, Berlin and Geneva, as well as in Washington, D.C. We are registered in the European Commission's Transparency Register (ID number: 502425118410-86.)

We appreciate the opportunity to submit comments on the General Data Protection Regulation (GDPR) guidance that the Working Party released on December 16, 2016. Our comments are on the *Guidelines on the right to data portability* (16/EN WP242).

The guidance issued by the Working Party reflects input from industry stakeholders on the challenges associated with implementing a data portability right. In many cases, we think that the Working Party has struck a reasonable balance in describing the conditions under which organizations give the data subject more control over his/her data, while noting that data portability guidance does not impose an obligation nor proscriptive technical standards on the data controller to retain personal data for longer than is necessary or beyond any specified retention period.

This letter seeks to offer additional perspective on the data portability right, the challenges of its implementation, and the balance between potential costs and benefits for consumers, and EU citizens.

The Feasibility and Economics of the Data Portability Right

SIIA agrees on the importance of enabling users to access their data in a structured, commonly used, and machine-readable format. We caution, however, against trying to require companies to make the data useful across divergent services. The vibrant marketplace of services which exists today results from the competition between technology companies on features and functions. Standardizing these features and functions would result in less variety and competition in the marketplace. Moreover, an effort, advertent or inadvertent, to require harmonization would likewise negatively impact the ability of small and medium sized enterprises (SMEs) to enter the

marketplace as they often serve niche markets or provide features and functions that are not commercially viable for larger multinational providers.

Firms that provide specific services are not in a position to transfer personal data for a data subject, but rather can make it available. Again, divergent features and functions will mean that not all features and functions will be portable or translatable. Companies will address these problems to some extent by agreeing upon industry standards, but at best these will operate as frameworks. Demand for portability solutions could be a rich opportunity for SMEs who can help support more complex portability requests, particularly when customers do not wish to take the time or effort to accomplish the transfer.

The primary rationales for the data portability right are empowering the individual, avoiding consumer "lock-in," and enhancing competition in the context of the digital single market strategy. As explained above, however, competition in the technology industry is driven by consumer demand for competing features and functions. This competition is undermined if data controllers are, for example, required to make application programming interfaces (APIs) available in every instance.[1] Indeed, the opposite would occur if standardization is to be required, or is an indirect outcome, to achieve interoperability between complex services and large data sets. Additionally, competition could be advanced if companies apply yet-to-be-defined industry standards developed within the European Interoperability Framework (EIF) to create new tools for data portability.

Portability Right Arises in Business to Consumer Relationships

The GDPR created the portability right in the context of a direct consent or a contractual relationship between a data subject and a controller (see Article 20). As such, we suggest that it would be useful if the guidance confirmed that the portability right applies only in a Business-to-Consumer context. Corporate employees who access a business service provided to their employer have no portability right to move their commercial usage history because they are accessing business, not personal, data. Instead, that history belongs to their employer, and rights to it are governed by B-to-B contracts.

Data Processors are not Liable for Portability Obligations of their Controller Customers

The Working Party's guidance does not appear to deal explicitly with the question of what to do when a data controller with a portability obligation engages a third-party processor to provide service on its behalf. For example, hospitals, app providers, and/or universities often engage data processing/cloud services companies, who may end up processing personal data on behalf of the data controller. However, those companies have no contractual or other relationships with the data subject(s) who have the data portability right. For example, a university retaining a company to run and maintain student records enters into a contract with a data processing provider which

[1] Peter Swire, Yianni Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Md. L. Rev. 335 (2013) The paper notes that the data portability right affects all companies, including small and other companies with no market power. Besides not being appropriate because competition policy seeks to limit monopoly power, i.e. typically large companies, potential costs of compliance are high and will ultimately inevitably be passed on to consumers, thus reducing consumer welfare. The authors point out, as well, the potential security implications of a consumer having a broad right to claim a lifetime's worth of data.

requires the provider to provide student data to the university upon request. This type of contractual provision would allow the university to respond appropriately to a student's request to transfer his or her personal data. The student's request should be submitted to the university, not the company processing her/his data. And if the student is dissatisfied with the results of her/his data portability request, the university (i.e., the controller) should be legally responsible. We would appreciate confirmation from the Article 29 Working Party regarding this matter.

Inferred and Non-Inferred Data

The Working Party appropriately says that a data controller "can exclude" inferred or derived data from the data portability right. However, the guidance goes on to say that the data portability right "should include all other personal data provided by the data subject through technical means provided by the controller."

Our view is that the only data that should be covered by the data portability right is data that is affirmatively provided by the data subject, not data that is generated passively through interaction with a website or an app. Consumers have a reasonable expectation to be able to retrieve what they actively and/or consciously provide, but they would logically not anticipate obtaining data passively generated through interactions with a website or app. Moreover, such "observed data" is typically gathered as a result of a consumer's use of a service and is, in fact, processed and analyzed and therefore inferred data that does not fall under the portability requirement. Also, this data is very often proprietary to the data controller. As a result, companies should make best efforts, but not be required, to include certain data generated at the direction of the data subject, such as financial calculations.

The Working Party appears to take this position in the paragraph in bold on page 9 of the guidance. We would appreciate confirmation on this point so as not to create the possibility of a class of inferred/derived data that is not covered by the data portability requirement and a class of inferred/derived data that is. Both should unequivocally be excluded.

Data Format Issues

As stated earlier, it is reasonable for the data controller to supply personal data to the data subject upon request "in a structured, commonly used, and machine-readable format." The discussion on the expected data format concludes by stating that "portability aims to produce interoperable systems, not compatible systems." It would be helpful for the Article 29 Working Party to clarify the Recital 68 statement. For example, one interpretation is that compatible systems involve identical schema and structures of personal data formats for the exchange of information that require no special interface to exchange information. It is not reasonable for each company to be obliged to use the same format to store data. Therefore, we agree with the conclusion of the guidance that the portability requirement does not mean that each firm must have systems that are compatible with the systems used by all other companies.

The Role of APIs

The Working Party states that data controllers "should offer a direct download opportunity for the data subject but should also allow data subjects to directly transmit the data to another data controller." The guidance suggests that this could be implemented by making an API available. We agree that interoperability is a goal to strive for, particularly where cooperation among industry stakeholders is possible, and that APIs are part of a resulting solution set. But an expectation that data portability produce interoperable systems is not always economically beneficial to consumers or companies. Interoperable systems usually mean that there is an interface (an API) that allows data stored in one system with a particular format to be transferred to a different system where it is stored in another format. This may be desirable in some instances, but there should be no expectation of an emerging blanket interoperability requirement. Competitors should not be forced to build interfaces for all possible permutations of marketplace participants and for all features and functions, because such a mandate would require every vendor to have its own API. Instead, it would be better to allow vendors to develop APIs from the common data formats or allow SMEs to create a cost effective "translation and transfer market."

Therefore, as the Working Party evaluates the implementation of the data portability right going forward, SIIA urges the Working Party to resist the notion that APIs should become over time a *de facto*, albeit not *de jure*, requirement. Small and medium sized enterprises (SMEs) would be negatively impacted if they are required to invest critical resources to create APIs for every circumstance, rather than investing in other data protection requirements. Although we believe data subjects will benefit from and should be provided with their data in a commonly used format, it should not be a data controller's responsibility to develop an API that works directly with the data formats of every possible competing data controller.

Anonymous and Pseudonymous Data

We note that the Working Party states that anonymized data is not subject to the data portability requirement. This is appropriate and consistent with the policy goal of anonymizing data.

The guidance further states that "pseudonymous data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier, cf. Article 11 (2)) is well within the scope" of a data portability request. But data that cannot be clearly linked to a person is not covered.

The GDPR incentivizes firms to anonymize and/or pseudonymize data and Recital 26 says:

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

Thus, the question is, if it is technically feasible to re-identify data upon request – no matter how time consuming, costly, or reasonable – should companies be obliged to do so? We believe that the answer is no. Rather, it is reasonable to take into account cost, time, and available technology

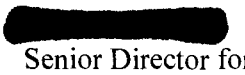
when considering data portability requests. And finally, when a data controller has anonymized or pseudonymized the data so that it cannot reasonably identify the data subject, the data portability requirement should not apply.

Personal Data Concerning Other Data Subjects

There is a strong analytical piece in the guidance with respect to personal data concerning other data subjects. SIIA agrees with the proposition that the right to data portability shall not adversely affect the rights and freedoms of others. We note, however, that requiring both "sending" and "receiving" data controllers to provide tools to enable data subjects to select relevant data and exclude other data subject's data would be costly to implement, especially for SMEs. Should the Article 29 Working Party insist on this requirement, there should be an explicit liability exemption for companies whose customers use data portability requests inappropriately.

SIIA takes the opportunity once again to thank the Article 29 Working Party for this opportunity to comment on the General Data Protection Regulation guidance for the right to data portability. We are at your disposal to answer questions and/or provide additional examples or information.

Sincerely,



Senior Director for International Policy
Software & Information Industry Association