Brussels, May 2020

BSA | The Software Alliance's submission to the ICO consultation on the Draft AI auditing framework guidance for organisations

BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the ICO consultation on the draft AI auditing framework guidance for organisations. The business-to-business (B2B) software industry is at the forefront of the development of cutting-edge innovation, including data analytics and artificial intelligence. Software-enabled technologies increasingly rely on data and, in some cases, personal data, to function to the benefit of business customers. As a result, the protection of personal data is an important priority for BSA members, and we recognize that it is a key part of building customer trust.

BSA would like to comment specifically on the portion of the ICO draft AI auditing framework guidance addressing the controller / processor relationship in AI and in particular in the context of "AI prediction as a service" (pages 23 and 24 of the draft guidance).

The distinction between controllers and processors is a key concept that has been part of the EU data protection legislative framework for over 20 years. Distinguishing between controllers, which determine the purposes and means of processing personal data, and processors, which process personal data on behalf of those controllers, including performing storage, processing, and other data

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cadence, Cloudflare, CNC/Mastercam, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

operations, is key to both allowing organizations that handle personal data to clearly define their responsibilities and to protecting the rights of individual data subjects. For example, as enterprise software companies, BSA members generally act as data processors under the GDPR by providing technologies and services used by other businesses that decide how to collect and process personal data. That may include storing data in the cloud on behalf of other companies, or providing software as a service tools that other companies can customize to suit their needs, without giving the processor visibility into the data run through those tools. However, BSA members may sometimes also act as controllers in certain circumstances. For instance, a company that operates principally as a data processor may nonetheless be treated as a controller under the GDPR when it collects data for the purposes of providing services directly to consumers.

Under the GDPR, controllers and processors have different levels of responsibility for achieving privacy outcomes that reflect their different roles. In particular, controllers have primary responsibility for satisfying certain legal privacy and security obligations and for honoring data subject rights requests. On the other hand, processors, which handle data on behalf of the controller to implement the controller’s objectives, are responsible for securing the personal data they maintain and following the instructions of a controller, pursuant to their agreements with relevant controllers. The processor/controller distinction not only provides organizations with a clear picture of their respective legal obligations, but helps to ensure that data subjects rights are adequately protected.

This key distinction should also be reflected in guidance relevant to AI. While AI tools will be used and deployed in a variety of different fields of human activity, BSA’s focus is primarily on the development of enterprise AI and its use in the business-to-business context, where the distinction between controllers and processors is a paramount concern.

In the context of enterprise AI, the tools that our companies provide are generally AI systems that facilitate human decision-making, without replacing human decision-making. With this in mind, it becomes clear that a company using an AI service to enable its employees to make a decision acts as a controller in deciding how and why that data is processed, and the AI system is used as a tool for processing data on behalf of that controller. Accordingly, the company providing the AI tool is appropriately treated as a processor.

We believe that the current draft guidance has the potential to blur the lines in the controller / processor relationship with regard to AI systems dedicated to prediction as a service. If read in that manner, the guidance could undermine this key distinction, which may create uncertainty for businesses that provide such services and undermine privacy protections for consumers.

1. **The draft guidance could be read to seek to requalify the entity that offers "AI prediction as a service," as a controller or co-controller of the data.**

The draft guidance suggests that a corporate customer may not be a controller when it uses an AI-based prediction as a service because in many cases "customers do not have sufficient influence of the essential elements and purposes of the processing involved in the prediction." That position is not consistent with the GDPR, which defines a controller as the entity that determines the "purposes and means" of processing data. In the context of prediction as a service, the customers clearly determine those purposes and means, and is therefore the controller.

We would like to stress that before an AI prediction as a service solution is deployed, the customer (controller) and AI developer (processor) will be engaged in contractual negotiations and in this context will clearly define and address the purpose of using the prediction system before the processing takes place. During this contractual negotiation, issues such as purpose, context, rights and obligations as well as expected outcomes and the explainability of the prediction as a service will be clearly addressed and endorsed by both the controller and processor. The Article 29 Working Party, in its 1/2010 opinion on the concepts of "controller" and "processor"[2] offers some helpful guidance in this regard: in section "III.2. Definition of processor", the Article 29 WP recognises that processors may establish standard processing terms without transforming their role into that of a controller. Specifically, the Article 29 guidance states:

> "*(…) it should be noted that in many cases service providers specialized in certain processing of data (for example, payment of salaries) will set up standard services and contracts to be signed by data controllers, de facto setting a certain standard manner of processing personal data. However, the fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself a sufficient*

[2] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

> *basis to conclude that the service provider should be considered as a controller, in so far as the controller has freely accepted the contractual terms, thus accepting full responsibility for them. In the same line, the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law."*

Even if customers who query the model via an API do not have the ability to configure the AI system, they determine the purpose of the processing of data and the means of processing – i.e., the decision to process the data via use of the API. Moreover, it is the customer that addresses obligations concerning the rights and obligations associated with the personal data used in the AI system, as well as providing instructions to the processor in the pre-use phase. In suggesting otherwise, the guidance appears to suggest that a controller must determine the "essential elements" of a service and defines those elements narrowly, including to include technical considerations like the ratio of false positives to false negatives.

As the GDPR recognizes, however, the question is actually broader, and focuses on whether a controller determines the "purposes and means" of processing. In making that determination, the Article 29 Working Party (in section "III.1.b) Third element: "purposes and means of processing"" of its 1/2010 opinion[3]) recognized under the Data Protection Directive that determining technical aspects of the means of processing does not transform a company into a controller. Rather, a controller's determination of the "means" of processing addresses key directional issues, such as "which hardware or software shall be used" and "essential elements which are traditionally and inherently reserved to the determination of the controller, such as 'which data shall be processed?', 'for how long shall they be processed?', 'who shall have access to them?', and so on." In contrast, as to more detailed decisions about technical aspects of processing, including scalable features which focus on important aspects, such as security, the Article 29 Working Party recognized that "it is well possible that the technical and organizational means are determined exclusively by the data processor."

[3] Ibid.

The European Data Protection Supervisor has endorsed this approach in its 11/2019 guidelines on the concepts of controller, processor, and joint controllership under Regulation (EU) 2018/1725[4]. In those guidelines, the EDPS specifically cited the Article 29 Working Party Guidance in recognizing that processors may decide the "more practical aspects of the processing operation(s)" without being transformed into controllers. The EDPS similarly recognizes that a controller is to determine "essential elements of the means" of processing, including the "type(s) of data to be processed, the period for which they would be retained, from which data subjects would the data be collected, who will have access to data (…) and the recipients of data (…)." In contrast, the EDPS recognizes that a processor may "identif[y] and determine[]" non-essential elements of the means of processing data "such as the software to be used or the technical and organizational measures that may need to be put into place, therefore assisting the controller in complying with its obligations under data protection law."

The requalification of the processor into controller, that the draft guidance seems to suggest, would be detrimental to the contractual relationship between controller and processor but also and most importantly to the privacy of the data subjects. Should AI companies offering APIs used for prediction services be considered controllers, they may be required to reach out to any individual whose data is processed via those APIs, to seek their consent or establish another lawful basis for processing. That result – of processors reaching out to individual data subjects – would overturn the protections afforded in the GDPR, by requiring companies that would otherwise not look at the data processed through those APIs to not only look at data relating to individual data subjects but also to contact those individuals. This would not only invade privacy of individuals, but likely be contrary to many contractual arrangements between businesses – since in many cases, customers of prediction services do not want processors reviewing their data absent exceptional circumstances and thus contractually prohibit processors from accessing that data. Aside from the contractual issues with accessing customer data for this purpose, it may also not be technically impossible for a processor to reverse engineer the data to identify the data subjects to whom the data pertains to.

Moreover, if the guidance were read to treat companies offering APIs used for prediction services as controllers, those companies may have to establish mechanisms to comply with data subject access requests, and potentially provide access to or correction or erasure of data used via those APIs. Again, doing this

[4] https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

may violate contractual terms – since companies offering such AI services may be prohibited from even accessing the underlying data, let alone providing access to others or altering or deleting it.   It would also require companies that process data to look at data they otherwise would not, undermining the privacy of that data. In addition, even if companies offering APIs used for prediction services were permitted to access the underlying data and provide it to data subjects in response to a rights request (and technically able to do so), adopting this approach may only create confusion among data subjects. For example, data subjects may have to submit requests to both the company using an API prediction service and the company offering that API prediction service, rather than making a single request to the company using the service. That could result in an individual that requested data only from the company offering the service mistakenly thinking that she requested to access, correct, or delete all relevant information. As the GDPR recognizes, the obligation to comply with data subject access requests properly falls on the company that decides how and why the data is used – in this case, the company that decides to use a prediction as a service API.

2. The draft guidance seems to consider that when a provider of an AI prediction service uses data to improve its service, it should be considered a controller

The draft guidance could also be read to suggest that where a provider of an AI prediction service uses data to improve that service, it should be considered a controller because it is processing the data for its own purposes.

Once again, we would stress that this interpretation would run counter to how controller/processor relationships have been understood and could lead to negative consequences not only for businesses that both use and offer AI prediction services, but also for data subjects. It is a well-established practice that a controller may instruct a processor to use data provided by the controller to improve the service provided by the processor. This practice benefits controllers, which receive better service as a result of that processing and are able to offer a better service to its own customers. Consistent with the GDPR, that processing is conducted pursuant to a contractual arrangement between the customer (controller) which collects and submits the data and the service provider (processor), which provides the AI prediction service. The controller accordingly continues to determine the purposes of this processing, by determining that data should be processed both to provide the underlying service and for purposes of improving the service.

Furthermore, if the ICO draft guidance is read to suggest that such a contract between the controller and processor would not be considered an appropriate legal basis for companies offering AI prediction services to process data to improve their service, it could create a scenario in which companies offering such AI services would have to identify and then seek consent from data subjects with whom they have no relationship, to establish another legal grounds for processing. That is contrary to the GDPR's recognition that individual privacy rights are to be addressed in the B2B context via a contract between controllers and processors that addresses each party's responsibility for honouring data protection obligations[5]. If the draft guidance contemplates that any processing of personal data for purposes of improving a product or service falls outside of these contractual protections, it would undermine the protections offered by the GDPR to the detriment of data subjects and may violate contractual restrictions designed to safeguard the privacy of information held by data processors.

This guidance may also keep companies offering AI prediction services from improving their AI models, if they cannot meet the obligations placed on a controller. For example, a company offering an AI prediction service could determine that it cannot honour data subject rights requests because it is contractually barred from accessing, correcting, or deleting data about particular data subjects. If the guidance were read to discourage that company from using data provided by a controller to improve its prediction service – even at the express direction of the controller seeking to use the service – it would be a bad result. AI technologies change quickly and regulators should encourage companies to create AI models that are as accurate as possible. Training the AI prediction services is also an important way to reduce bias, an important element that was recognized by many data protection regulators, including the UK ICO, in the declaration on Ethics and Data Protection in Artificial Intelligence adopted in 2018[6]. Restricting the ability of providers to update AI systems may also have a detrimental impact on the safety and security of those services. The guidance could be read to discourage such improvements and instead err on the side of discouraging improvement, resulting in a potential trade-off favouring less accurate and secure technologies without improving significantly personal data protection. To the extent that companies

[5] Article 28 paragraph 3 of GDPR: *"Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. (…)"*

[6] https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdf

cannot improve AI systems without being treated as controllers in a particular jurisdiction, it may ultimately decrease incentives to deploy new technologies in those jurisdictions and create a more fragmented marketplace with disparate access to new products and services.

We would welcome the opportunity to engage further with the ICO on the issues highlighted above.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315