Brussels, November 2021

# BSA | The Software Alliance

## Submission to DCMS on Consultation for Data: A New Direction

BSA | The Software Alliance (BSA),[1] the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the UK Government's consultation on potential reforms to the UK General Data Protection Regulation (UK GDPR). Our members are business-to-business companies that create the technology products and services that power other companies, including cloud storage services, customer relationship management software, identity management services, and workplace collaboration software. These enterprise software companies are in the business of providing privacy-protective technology products. BSA members recognize that they must earn consumers' trust and act responsibly with their personal data.

We appreciate efforts by the Department for Digital, Culture, Media & Sport (DCMS) to recognize the practical ways in which high standards of data protection may be maintained while encouraging the responsible development of technologies.

Our comments focus on five aspects of the consultation:

1. Interoperability.
2. Transfer Mechanisms.
3. Legitimate Interests.
4. Data Breach Notification.
5. Artificial Intelligence.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. 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. Follow BSA at @BSAnews.

BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

## I. Importance of Interoperable Laws That Maintain High Standards of Data Protection

As countries worldwide develop or update their personal information protection laws and regulations, it is critical that those frameworks are designed to effectively protect privacy in a manner that is internationally interoperable, flexible enough to account for rapid evolution in both technologies and business models – and prioritizes high standards of data protection.

Of course, the context and perspective around privacy and personal data protection may appropriately vary among different countries based on cultural expectations, legal traditions, and other factors. At the same time, governments must strive to support the common recognition of international norms and practices around core aspects of personal data protection, which underpin interoperable privacy frameworks. The emergence of fragmented policies on core issues of data protection raises the cost of business for all companies and can undermine personal data protection and consumer privacy. Although governments often focus on the need for interoperability in the specific context of data transfers, we want to emphasize the need for interoperable approaches to data protection is far broader – and substantive interoperability among data protection frameworks is paramount in facilitating organizations' ability to comply with requirements across jurisdictions.

In this regard, we encourage the UK Government to remain cognizant of the resources that many organizations have expended on developing an internal privacy framework that is consistent with the requirements of global data protection laws, including both the UK GDPR and the EU GDPR. We appreciate the UK Government's efforts to recognize that existing measures taken pursuant to the UK GDPR and the EU GDPR would likewise satisfy any new requirements under UK law. In addition, the UK Government should only introduce new data protection obligations if their objectives are distinct from the goals and objectives of existing global data protection laws; this would help avoid, as having duplicative obligations that may simply increase the resources that organizations need to expend on privacy compliance without a corresponding increase in meaningful privacy protections We also appreciate the UK Government's recognition of the importance of maintaining interoperability between the UK's data protection regime and the legal regimes of other jurisdictions. By supporting an interoperable approach to data protection, the UK can help to create a coherent environment for businesses that seek to operate internationally. It can also help avoid contributing to a fragmented approach to data protection that may ultimately harm the ability of organizations to do business in the UK. In this regard, we welcome the UK Government's focus on ensuring the UK data protection framework can be practically applied by organizations conducting business both in the UK and beyond its borders. We further recommend that the UK Government support interoperable approaches to data protection by publishing practical guidance regarding the circumstances for which compliance with the standards imposed by other governments, including EU standards, fulfill UK requirements.

The UK has a unique opportunity to prioritize an approach to data protection that is practical in nature, interoperable in practice, and soundly committed to maintaining high standards of data protection and we encourage you to do so in a manner that embraces the importance of global interoperability.

## II. Need for Strong Set of Transfer Mechanisms

We welcome the consultation's recognition of the importance of cross-border data flows. The UK will set important global precedents as it reflects on the future of transfer mechanisms. At a time of rising

protectionism across the world, the UK should continue to promote strong privacy safeguards and international data flows as pillars of the data economy. The UK should also be a strong voice against localization trends and other restrictions to international data flows. This work is crucial in at least two respects:

- ***First, the ability to transfer data, including personal data, across international borders is the lifeblood of the modern digital economy.*** Companies in all industries require the ability to transfer data across international borders. In sectors as diverse as agriculture, healthcare, manufacturing, and banking, businesses that produce a broad range of products and services are united by the need to send data across international borders. Everyday technologies like cloud storage services, customer relationship management software, human resource management programs, identity management services, workplace collaboration software, cybersecurity solutions, and supply chain management services all depend on the ability to transfer data across national boundaries. Cross-border transfers are also vital to consumers and workers who expect to use global services that connect them with others worldwide in a manner that protects the privacy and security of their data.

- ***Second, companies require a range of transfer mechanisms to support global data flows – and those mechanisms must be built on strong data protection safeguards***. We support the UK's efforts to ensure that organizations have several practical options to use in transferring data across international boundaries, including adequacy determinations, standard contractual clauses such as the proposed IDTA and addendum, and other mechanisms. Different types of organizations and different business models require the use of different transfer mechanisms that are not interchangeable. In practice, larger companies will often rely on one or more data transfer mechanisms, using the tool most tailored to their business needs and to the specific data transfer(s) at hand. Other businesses may principally rely only on one mechanism, such as adequacy determinations or standard contractual clauses.

We welcome the UK Government's focus on supporting a broad set of transfer mechanisms and offer views on several of the mechanisms highlighted in the consultation:

- **Adequacy (Q3.2.1, Q3.2.3).** We welcome the UK Government's focus on adequacy assessments (or Data Partnerships) as providing a strong and durable transfer mechanism and are supportive of the government's intention to progress an ambitious program of adequacy assessments. We also appreciate the government's intention to approach adequacy assessments from a practical perspective, but want to emphasize that in doing so the UK should continue prioritizing strong data protection standards as the basis for durable adequacy assessments. This is important not only for the UK's own reputation but also to ensure that the UK maintains its own designation of adequacy from the EU. The UK's adequacy determinations can contribute to global convergence by informing other countries addressing similar issues under their own data protection frameworks. They will also provide UK organizations with a valuable alternative mechanism for transfers to Data Partnership countries and we welcome the UK's publication of a list of countries for which it intends to prioritize adequacy partnerships. Going forward, we encourage the UK to continue determining priority countries based on guiding criteria that reflect the relevance for business and on the country's commitment to strong values of data protection.

- **Alternative Transfer Mechanisms (Q3.3.2).** As noted above, the UK should continue to ensure a robust international transfer regime that recognizes multiple stable and trusted mechanisms for companies to transfer data across international borders. While adequacy determinations can be one important mechanism for supporting international transfers, we want to emphasize the need to ensure other mechanisms continue to support international transfers. In this regard, we welcomed the ICO's recent consultation on data transfers, including its publication of both the standalone IDTA and the IDTA in the form of an addendum, the latter of which is of significant practical value to companies.

- **Certification Schemes for International Transfers (Q3.4.1 - Q3.4.2)**. In addition to focusing on transfer mechanisms based on adequacy determinations and standard contractual clauses such as the proposed IDTA and addendum, we appreciate the UK Government considering modifications to the framework for certification schemes. We agree with the consultation that such schemes can provide a more globally interoperable and market-driven system. In connection with potential reforms, the UK Government is considering clarifying that certification bodies outside of the UK may be accredited to run UK-approved international transfer schemes, which it envisions would encourage existing international programs to engage with UK standards bodies to develop UK compliant schemes to support data flows with UK businesses. BSA supports this type of voluntary certification scheme, which can provide companies with additional accountable mechanisms to transfer data across borders. We also applaud the UK Government for recognizing the need for certification schemes to work with bodies outside the UK. In this respect, we want to emphasize that certification schemes are most useful for organizations when they are recognized and adopted by more than one jurisdiction – and thus can permit companies using a single certification scheme to comply with obligations in multiple jurisdictions. We encourage the UK Government to prioritize these practical benefits in focusing on the use of certifications as transfer mechanisms.

## III. Grounds for Processing and Specifying Legitimate Interests (Q1.4.1-1.4.3)

We welcome the UK Government's continued recognition that data protection frameworks should not place more reliance on consent than on other bases for processing personal data and see this as fundamental to a pragmatic and commercial data protection regime. We also applaud the UK's efforts as a strong proponent of other lawful grounds for processing, and its recognition that a number of common place scenarios may involve appropriately processing data without seeking an individual's consent. For instance, organizations rely on legitimate interests as a basis for processing data about their network in order to improve security and guard against fraud. These positions will be critical as the UK Government leverages its role in the international conversations around developing privacy protective data protection frameworks. Indeed, there is widespread recognition that consent-based frameworks may increase burdens on data subjects (with little benefit to them) and lead to consent fatigue, because they may require data subjects to provide consent to many types of processing they already expect, such as processing to deliver the goods and services they request.

The consultation also proposes clarifying the legitimate interest grounds for processing, in part to incentivize organizations to use all appropriate legal grounds available to them. In particular, the consultation notes that organizations may be dissuaded from relying on legitimate interest grounds for

processing because it requires not only that processing be necessary and proportionate, but a balancing test assessing how the organization's interests outweigh the rights of data subjects. Rather than require organizations to conduct this balancing test in all scenarios, the consultation proposes an exhaustive list of situations in which the Government concludes that the balancing test favors organizations. The consultation lists several scenarios that could be identified on a limited set of legitimate interests, including monitoring, detecting or correcting bias in relation to developing AI systems, improving an organizations' system or network security, and internal research and processing that improves customer services.

We encourage the UK Government to focus on two considerations in determining whether to list out such legitimate interests in legislation:

- *First, the practical impact of such a change*. In practice, legitimate interests are already noted in the ICO guidance as an appropriate legal basis for many of the items on the consultation's proposed list. Indeed, the ICO's current guidance on application of the legitimate interest grounds and the UK GDPR's recitals recognize that fraud prevention, ensuring network and information security and indicating possible criminal acts or threats to public security constitute a legitimate interest. As the ICO notes, the recitals to UK GDPR also identify three other activities that "may indicate" a legitimate interest: processing employee or client data, direct marketing, or administrative transfers within a group of companies. We encourage the UK Government to seek industry's feedback to gauge the expected practical impact this measure could have on different business models and different types of organizations, given that the impact of the proposed change to legitimate interests may be limited in light of the current ICO guidance. In particular, the UK Government may consider the extent to which removing the requirement to conduct a legitimate interests balancing test reduces the administrative burden on companies in practice, since they are still required to ensure processing is necessary and proportionate.

  In addition, another practical consideration is the extent to which any list of legitimate interests will take into account the evolution of business models, technology, and data subjects' expectations, all of which inform the way organizations rely on legitimate interest. Therefore it would be beneficial to ensure that any such list remains a living document.

- *Second, the need for clarity in applying the list.* As set out in the consultation, some of the situations on the proposed list of legitimate interests could be interpreted quite broadly. While this may provide flexibility for organizations and reduce over-reliance on consent, any such list should also be carefully crafted to ensure it is applied in a manner that respects the strong data protection values embodied in the UK GDPR.

## IV. Threshold for Breach Reporting (Q.2.2.12)

The consultation proposes changing the threshold for reporting a breach to the ICO, so that only *material* breaches are reported. The consultation also proposes encouraging the ICO to create guidance and examples of non-material risks that would not require reporting.

BSA members strongly welcome this proposal. Globally, BSA supports reasonable and appropriate personal data breach notification requirements – including a risk-based notification standard that focuses reporting and notification requirements to instances in which there is a material risk of harm.

As the consultation notes, the current requirement to inform the ICO of a data breach unless it is "unlikely to result in a risk to the rights and freedoms of natural persons" sets a threshold that creates incentives for organizations to over-report potential incidents. We appreciate the consultation's recognition of the costs of over-reporting, which can not only create additional work for the ICO to understand situations in which consumers are not exposed to material risks, but also can distract consumers and organizations from focusing time and resources on higher-risk scenarios.

We also support the consultation's suggestion to encourage the ICO to produce guidance and examples of risks that are not material, to create additional clarity around these obligations. In particular, such guidance may appropriately recognize that no material risk to individuals arises when the personal data at issue is encrypted or redacted. Because the data could not be accessed if it is encrypted or redacted, no material risk to an individual would be created. In addition, where possible and in line with our recommendations on interoperability of regimes set out above, it may again be helpful to identify the circumstances in which when compliance with the data breach obligations imposed by the laws of other governments may satisfy this UK requirement.

## V. Artificial Intelligence

Finally, we appreciate the UK Government's recognition of the importance of developing trusted and responsible artificial intelligence technologies. We agree that a data protection framework can help organizations building or deploying AI tools to innovate responsibly, manage data-related risks throughout the AI lifecycle, and ensure that individuals can trust their personal data is used responsibly.

Although the consultation touches on a range of important AI issues, we want to highlight two topics critical to data protection regimes that support trusted AI development:

- **Importance of Testing For and Mitigating Biases (Q1.5.5, Q1.5.10)**. We particularly welcome the UK Government's focus on ensuring that developers and users of artificial intelligence are encouraged and permitted to test those systems for potential biases, which helps organizations identify and mitigate potential risks through the AI lifecycle. This issue is a priority for BSA members, which work hard to ensure the technologies they develop are used in trusted and responsible ways. In response to the risk of bias, BSA recently published a report titled "Confronting Bias: BSA's Framework to Build Trust in AI" to provide a guide that organizations can use to perform impact assessments to identify and mitigate risks of bias that may emerge throughout an AI system's lifecycle. We welcome the UK Government's focus on these issues, including its proposal to treat testing for bias as a legitimate interest. As set out above, to the extent the UK Government adopts such an approach to specifying a list of legitimate interests for which no balancing test is required, we encourage the government to further consult stakeholders on how this approach is most beneficial in practice and paired with sufficient guardrails to ensure it is applied in a manner that prioritizes strong data protection standards.

- **Importance of Context in Assessing Fairness (Q1.5.1- 1.5.4).** The consultation also highlights the importance of fairness in considering AI systems and the complicated nature of understanding how the broad concept of fairness applies to AI. We appreciate the consultation's recognition that there are many different lenses through which to view fairness, including fair uses, procedural fairness, and outcome fairness, and the UK Government's recognition that fairness is necessarily both "broad and context-specific." In practice, applying the principle of fairness to AI systems requires developers to evaluate the nature of the system they are creating to determine which metric for evaluating bias is most appropriate for mitigating the risks that it might pose. It can also require companies using AI systems to carry out an assessment of those uses and take the appropriate mitigation measures, depending on the context in which the AI systems is effectively being used and for which purpose. In some circumstances, it may be impossible to simultaneously satisfy all fairness metrics, making it necessary to select metrics that are most appropriate for the nature of the AI system that is being developed. As the UK Government further considers these issues, we encourage you to consult broadly with a range of stakeholders that may provide insight into the many contexts in which fairness underpins considerations around the development and use of AI technologies.

## Conclusion

Effective data protection is an essential component of trust in the digital economy; it is also an important priority for BSA members. BSA is grateful for the opportunity to provide these comments and we would welcome the opportunity to engage further with the UK Government on these issues.

---

For further information, please contact:

Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315