5 January 2023

Re: Comments Pursuant to Recommendation 1/2022 Concerning Binding Corporate Rules

The Information Accountability Foundation (IAF), a non-profit organisation whose purpose is research and education, respectfully submits the following comments related to the Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of the European Data Protection Board (Recommendations).

Binding Corporate Rules (BCRs) were put forward by the Article 29 Working Party in 2004 as a means for certifying that personal data transferred by a controller would be protected at the same level as it would be protected within the European Union. Before the first BCR approvals took place, the accountability principle was further defined by the Global Accountability Dialog[1] and then as an opinion in 2010 by the Article 29 Working Party. By that point, BCRs had become a means for controllers to certify that they were fully accountable organisations. The BCR approval process became a window into the privacy processes at organisations that sought certification and would remain so according to the changes to the application form set forth in the Recommendations. So, the value of BCRs moved beyond the initial purpose of being a mechanism for transfers to also being a means for the European data protection enforcement community (DPAs) to have better transparency into benchmark corporate data protection programs. Organisations have taken extra steps for BCRs, beyond other less rigorous transfer mechanisms, because the certification is a ratification of a sound data protection program. BCRs have been expensive and time-consuming both to seek and expensive and resource intensive to approve, but they have provided a value beyond just legal certainty for transfers. It is useful to preserve this added value, beyond transfers, that BCRs bring to individuals, groups of people, regulators, and organisations. The IAF is concerned that Section 4 of the application form, the Acknowledgement, will make BCRs impractical for many organisations that already have BCRs. There still will be organisations where the reputational value of BCRs will be attractive enough but will there be enough organisations to have the critical mass for the learning purposes of BCRs.

Section 4 requires the controller to acknowledge that it understands the responsibility to conduct an assessment of the law in the destination country to see if there are impediments to complying with the requirements of the BCR. The language then goes on to require the data exporter, if necessary, with the help of the data importer, to "ensure an essentially equivalent level of protection as provided in the EU." This standard is the same as the GDPR adequacy requirement for the EU Commission contained in Article 45 of the GDPR, which is essentially equivalent laws, not the standard contained in Article 46.

[1] The Global Accountability Dialog was an independently funded project of the Centre for Information Policy Leadership. That project was incorporated in 2013 as the Information Accountability Foundation. Martin Abrams, one of the authors of these comments, was the CIPL president when the dialog took place, was the project leader, and the first president of the IAF.

Article 46 provides that the supplementary measures when there is no adequacy decision under Article 45(3) include Standard Contractual Clauses and BCRs. The standard under Article 46 is, for European individuals, the enforceability of rights and effectiveness of legal remedies. The question is not whether the laws are equivalent, which is a responsibility for the EU Commission, but rather whether personal data of a certain type will be subject to bulk collection by law enforcement and national security from the importer, and whether European individuals have enforceable rights and effective legal remedies if that happens.

The Standard Contractual Clauses permit and provides guidance for assessing the Article 46 risk of data being used beyond the individual's ability to exercise rights. Footnote 12 in Clause 14 of the Standard Contractual Clauses states:

> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

This is further discussed in a blog published in the IAPP Advisor entitled "Confusion about the meaning of 'Schrems II' Impedes Global Data Flows" by IAF Senior Strategist Lynn Goldstein.

The EU Article 29 Working Party provided definition to risk and risk management in a 2017 opinion "Guidelines on Data Protection Impact Assessment {DPIA} and determining whether processing is "likely to result in a high risk" for purposes of Regulation 2016/679" (GDPR). The opinion says "a risk is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. Risk management, on the other hand, can be defined as the coordinated activities in direct and control an organization with regard to risk." The opinion also provides guidance on what is meant by the risk to fundamental rights and freedoms, saying that it is primarily reserved to risks against data protection and privacy, but not limited to them. Practical experience since 2017 demonstrates that the risks to individuals from the processing of data goes beyond privacy and data protection, and maybe, in some instances, other risks have greater weight.

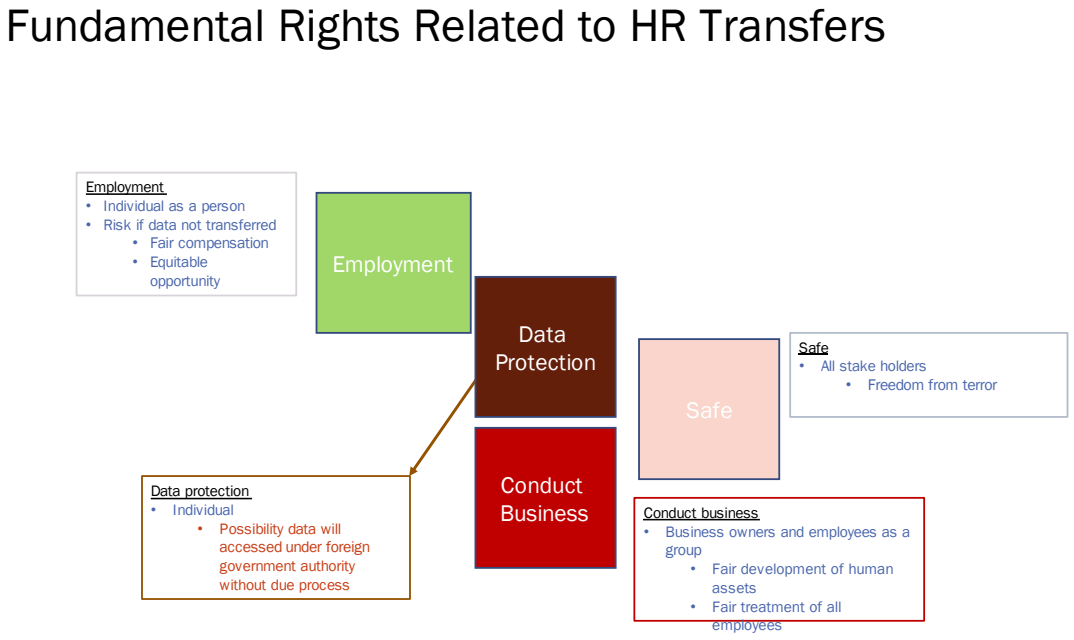
The GDPR reserves DPIAs for high-risk processing. Schrems II expands the circumstances where there is high risk to when personal data is transferred to a third country. The IAF believes this risk assessment should take into account not only where the data is transferred, but also the types of data being exported and the actual likelihood of that data being subject to bulk collection. This issue was specifically explored in the IAF 2021 paper "Addressing Human Resources Data Flows in Light of

European Data Protection Board Recommendations." This paper was updated in August 2021 when the EU adopted new standard contractual clauses.

There are very few absolutes in data protection. That is why the GDPR is intended to be risk based. Recital 4 states clearly that data protection is not absolute and that rights to data protection must be balanced against other fundamental rights and freedoms. When more than one fundamental right is being considered, the likelihood and the severity of the consequences of an adverse processing impact taking place and who those adverse processing impacts might affect need to be looked at.

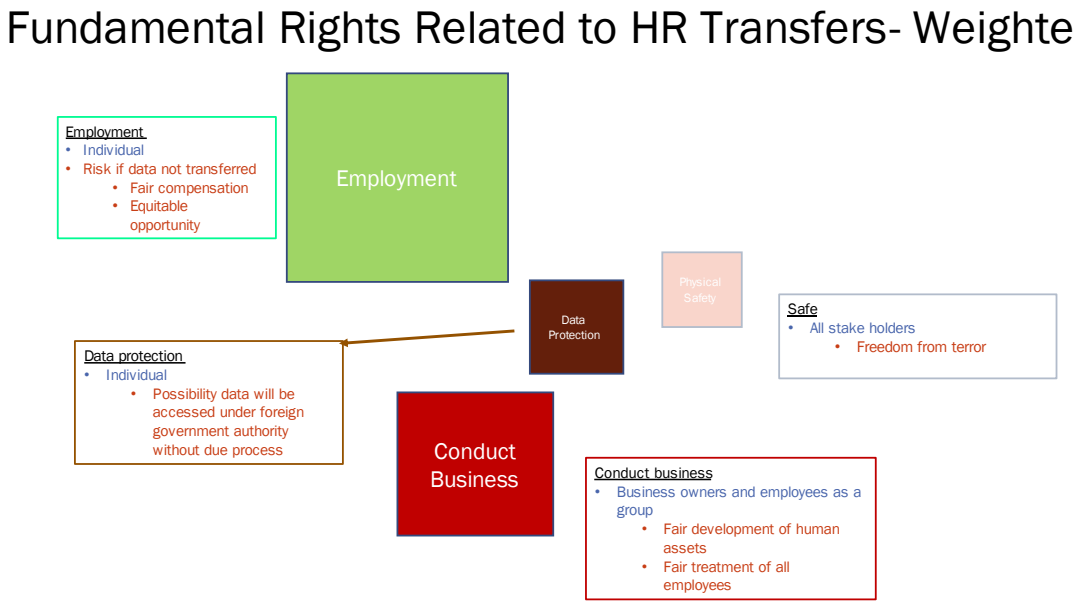
For the past two years, in a project entitled "Risk of What? ", the IAF has been exploring the nature of risk in data driven ecosystems and who is impacted by those risks. That project led to the conclusion that there are many stakeholders impacted by the processing of data, and that it is useful to graphically chart who those stakeholders are and how they are impacted. This conclusion further led to a an IAF project on how to broaden the proportionality principle so that it could encompass numerous risks and stakeholders. That work in ongoing. However, an interim paper was issued 12 December 2022 entitled "A Principled Approach to Rights and Interests Balancing – Multi-Dimensional Proportionality." The following charts come from that paper.

The IAF previously had conducted research on the flows of data that support employee evaluation and similar human resource activities. The EU Charter of Fundamental Rights defines numerous rights. The IAF explored how they might be impacted when data flows across borders to support employee evaluation. They include the rights to data protection, have an occupation and engage in work (employment on the chart), conduct business, and be safe.



The IAF found no instances of the type of HR data used for evaluations being subject to bulk collection by law enforcement or national security agencies. So, the likelihood of that risk was unmeasurable. On the other hand, the inability to review data related to individual performance could impact employees in

numerous ways. The absence of that data went beyond the individual employee to other employees that are competing for pay increases, other remuneration, and even job retention. Lastly, the organisation is impacted by the lack of fair treatment for employees. These impacts particularly could affect protected classes of employees. So, in weighing the likelihood and severity of the fundamental rights in consideration, the IAF generated the following chart.



The IAF has concluded that Section 4, Acknowledgement, requires an organisation to conduct an Article 45 assessment on adequacy, rather than the Article 46 assessment that is required for Supplemental Measures. Applying the Article 45 "essentially equivalent" standard to BCRs, rather than the Article 46 "enforceability or rights and effectiveness of legal remedies" standard which is applied to Standard Contractual Clauses makes BCRs a less desirable supplementary measure. The Article 45 assessment should not be placed on private sector companies who have BCRs. The higher-level requirement for BCRs might make the process less attractive for organisations. If less organisations have BCRs the data protection enforcement community would lose market intelligence.

Any questions should be directed to Martin Abrams at mabrams@informationaccountability.org.