The CPH appreciates having had the opportunity to work with the small team on reviewing the authorization provider building block, and looks forward to further review with the plenary group at our upcoming meeting.

This building block is structured as an assessment that guides its reader through making the disclosure decision. However, it is not reasonably possible to provide enough specificity for such a templated assessment process to succeed.

Each request has individual context that must be considered, including varied and evolving international laws applicable to the data subject and requestor, as well as the unique circumstances of each request. This would be very difficult to itemize and translate into templated options from which the authorization provider would select. As confirmed in the Bird & Bird Liability, Safeguards, Controller & Processor Memo, setting up rules for disclosure requires significant care. Even if we can determine categories of requests, "it might not be safe to assume that for such a bucket, the balance of legitimate interests is always in favour of disclosure, as this could be affected by the status of the data subject or the country in which the law enforcement body is located."

Additionally, the risks of making an incorrect decision are extremely high, and, as identified both by the EPDP team in the Automation building block and by Bird & Bird in their Legitimate Interest and Automated Submissions and/or Disclosures memo, automation is frequently not an option available to the authorization provider. For example, if a data subject objects to being subject to a decision based on automated processing under their GDPR Art. 22 right, how would that be conveyed to the SSAD operator or authorization provider? As such, automation is certainly possible and achievable for the request submission process, but meaningful human review of many, if not all, requests is required, even if only to determine if a request is eligible for further automated processing because it relates only to non-personal data.

Other points of further consideration for this Building Block include how it relates to our Logging Building Block, specifically since logs created by the authorization provider are also subject to data privacy regulation and can themselves be Personal Data (see B&B Liability memo 3.14), as well as considerations around cross-border data transfers. B&B indicated in the Liability memo section 3.17 that the EPDP expects to rely on Standard Contractual Clauses (SCCs) to protect the data. However, B&B point out that some requestors will refuse to be bound by SCC's, the exporter also has significant and potentially difficult obligations around ensuring that the recipient can satisfy their legal obligations, and finally, the Controller/Processor relationship needs to be clearly defined, as "all forms of SCC available today are premised on the data exporter being a controller established in the EEA."

By working collaboratively through the Authorization Provider Building Block in the small team we have discovered that we need to focus on creating a set of guidelines for the authorization provider to follow, rather than a templated evaluation. There is an alternate possibility, entirely dependant on the Model that is ultimately confirmed to be the most compatible with the potential

pending guidance from the EDPB, that an independant SSAD provider who is also the sole Controller should more appropriately develop such evaluation criteria in collaboration with their own independent legal counsel, and therefore should not be restricted by a dicta of the EPDP team. All these considerations will then allow the EPDP team to standardize the requestor's experience and level-set our expectations of the SSAD operator and authorization provider without restricting ourselves to a process that only sets us up for failure down the road when it is found to be inadequate.