LVMH

*16 December 2020*

**LVMH Contribution to the Consultation on the EDPB Recommendations 01/2020**

**General comments:**

- The supplementary measures identified in the EDPB Recommendations, including in particular encryption with a key owned and managed exclusively by the exporter (BYOK), may take a long time to implement in practice, as it does not correspond to current general industry practices. We consider that these supplementary measures proposed by the EDPB are very protective of personal data, but we need to have sufficient time to determine and put all these measures in place with our providers. **A reasonable transitional period** needs to be provided to allow companies to become compliant.
- From a general standpoint, we consider that in the current version of the Recommendations, most of the obligations are put on the data exporter, whereas we believe that **both parties, exporter AND importer, should be held liable and responsible for determining and putting in place relevant supplementary measures**.
- **The Costs of the supplementary measures** should also be taken into account. Importers should not exploit the situation and over-invoice the exporters due to these new measures.
- It cannot be the **data exporter's responsibility to assess third-party countries' local laws**. Data exporters cannot assess all local laws around the world and need to rely on (i) the data importer (which is located in the third-country or provide the services from this country and is therefore supposed to know the laws applicable to its business) or (ii) the supervisory authorities/European Commission/EDPB which can provide official assessments. An assessment by supervisory authorities/European Commission/EDPB would avoid discrepancies between assessments for similar situations and would therefore ensure effective and consistent protection of transferred personal data for all data subjects.
- **CISO is a key stakeholder** to contribute in determining the adequate technical measures to discuss and implement. It could be valuable to highlight this role in the Recommendations.

- It is mentioned several times that: "*transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.*". Transport encryption is ensured by Certificate Authority acting as a trusted third party—trusted by both data exporter and data importer. **It is only encryption at-rest that can be achieved by using a key that would be owned exclusively by the data exporter**. Besides, this can be achieved, if and ONLY if, the service can be performed with such a condition, which is not always the case. Indeed, this implies in practice that the application can decrypt "on the fly" the data (the private key is set up in the application and the data importer does not have sufficient permissions to access it) with the appropriate IT computing resources to perform the operations in an efficient way (CPU/RAM/Storage). There is a topic about encryption in-use, for database engines for instance … and also the principle of encryption "without any break" which need to be addressed.
- **Data masking** is another method that can ensure an adequate level of protection and which could be mentioned in the Recommendations. Developing additional levels of granularity in user's rights and permissions would make it possible to adapt the availability of data to what is strictly necessary for the user to accomplish his or her task.