Deutsche Post Dialog Solutions GmbH
Classification of data criticality
V.1 February 2024

Dear Client,

We take care for your data with responsibility and sensitivity. In accordance with article 32 GDPR we implement appropriate technical and organizational measures in context and purpose of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. We like to provide a protection level appropriate to the risk concerning confidentiality, integrity, availability, and resilience of the systems in due consideration of the state of the art, implementation costs, the nature, scope, and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Art 32 Paragraph 1 GDPR. According to your order requirements and the above mentioned we diligent choose the most appropriate subprocessor from our portfolio.

In order to accomplish the above mentioned and **prior to processing** we ask you to classify your data into the subsequent risk classifications (data criticality): „**low**“, „**medium**“, „**high**“ or „**very high**“ . For more information regarding data risk classification please see below stated scale. Furthermore, we ask you to inform us prior to processing when your data **belong to the special categories of personal data** (e.g. health, marital Status, union membership, political opinions, racial and ethnic origin, religious or philosophical belief/conviction, genetic or biometric data) according to Art. 9 and/or 10 GDPR.

Please note: In case of not having any classification information from you we consider your data classification as „low”.

Personal data	Examples (Please note: Data and or risk aggregation can lead to a higher risk classification!)	Severity of potential damage/impairment	Data risk classification
opened to public by data subject itself.	**E.g. name and address for direct marketing purposes.**	insignificant/negligible	**low**
whose improperly processing causes no special impairment, but was not opened to public by data subject itself.	Limited access to open data, e.g. inspection to the land register, not open accessible social media data, masked IBAN (last six numbers blacked), client master data, birthday, place of birth.	Insignificant/negligible	**low**
whose improperly processing could lead to impairments of social position or economic status of data subjects.	Income, tax data, infringements of law, passport specifics, unmasked IBAN , contract data (e.g. delivery date).	manageable	**medium**

whose improperly processing could lead to severe impairments of social position or economic status of data subjects („threat to existence”).	Commitment to an institution, personnel reviews, certification of employment, health data, debts, distraints, special categories of data according to Art. 9 GDPR.	substantial	**high**
whose improperly processing could cause impairments of life, health or freedom of data subjects.	Crime delinquencies, data about people being potential crime victims, witness-protection programs.	huge	**very high**