OUR DATA PROCESSING CODES

*This fact sheet is part of Crayon's proactive communications strategy on **Information Security and Data Protection (ISDP)**.*

This fact sheet aims to provide you with a concise summary of Crayon's **Data Processing Codes**, which are applicable to current team member, contractors, consultants, agency staff and applicants.

To enable you to process restricted data (incl. personal data) securely on our IT systems, you will receive mandatory training and a copy of our *IT Use and Data Processing Policy*. In addition, you will receive a copy of those *Processing Guidelines* which govern the proper handling of restricted data in relation to your function. As an integral part of our information security and data protection culture, we also expect you to ensure you are up-to-date on training related to your role and responsibilities.

For further information, please contact our Data Protection Officer (DPO): dpo@crayon.com

Our Privacy Principles

Our commitment to safeguard privacy when processing personal data is grounded in *Crayon's 7 Privacy Principles*:

1. Personal data will be **processed lawfully and fairly**.
2. Personal data will be **kept, used, or disclosed only for specific and lawful purposes**.
3. Personal data will be **adequate and relevant, not excessive**.
4. Personal data will be **retained for no longer than is necessary for the purposes for which they were obtained**.
5. Personal data will be **accurate, complete, and up-to-date**.
6. Personal data will be **provided in transcript copy to individuals upon request, in line with our commitment to the law**.
7. Personal data will be **kept secure using technical measures and organisational measures, grounded in privacy by design**.

***Data Processing**: collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making available, erasing or destroying (Art. 4(2) EU GDPR).*

***Personal Data**: Any information relating to an identifiable person (data subject) who can be in-/directly identified by reference to an identifier – e.g.: name, an identification number, location data, an online identifier – or one/more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity (Art.4(1) EU GDPR).*

Our Data Classification

Data is made available to intended audiences depending on our distinction between four levels of data sensitivity:

Public Data	Is available to external and internal audiences without any discretion.
Private Data	Is available ONLY to the data creator/owner and this data may NOT be made available to any other person, except in accordance with the instructions of the data owner.
Internal Data	Is made available to all team members, but is not to be disclosed to any external person, except in accordance with the predefined rules issued by Crayon or the explicit permission of the Head of Information Security.
Confidential/ Personal Data	Is made available to you on a need to know basis. This may be based on your job description or enabling you to carry out an assigned task. Collected or generated by us, our customers, partners or suppliers, this data may NOT be made available to unauthorised team members or external parties without the written permission of the data owner.

Your Responsibilities: During your employment and upon end of contract you must:

- **Keep internal and confidential data secure**.
- **Do NOT use any restricted data**, except as authorised by us for the purposes of your job.
- **Do NOT disclose Internal/Confidential Data** – *exceptions: authorised under our procedures or permission of the data owner*.
- **Seek guidance if you are unsure** about data classification or sharing from your supervisor or DPO.
- **Read and understand the *Processing Guidelines*** which are applicable to your duties.
- **Ensure you abide by our *Crayon's 7 Privacy Principles*** when processing personal data.