Dentsu approach to data protection

Our Global Data Protection Principles

As leaders in data, technology, and creativity, the work we do is woven into the lives of millions of people across the world. We have the opportunity, privilege, and responsibility to use our powers for the lasting good of everyone.

Our approach to data protection across dentsu reflects the standards and values set out in our Code of Conduct.

Being a *force for good* is one of dentsu's universal ideals – the "8 ways to the never before" - that guide our people and permeates everything we do.

If we want to create truly sustainable value for the organisations we work with, to be trusted partners and have the power to do good for the people and the communities in which we work and live, then we must treat people and their personal data carefully and with respect.

The dentsu Global Data Protection Principles guide our understanding of what being a force for good means in the context of personal data processing - regardless of where in the world we may operate. These principles underpin the policies, standards and behaviours that govern how we collect, use and work with personal data across the dentsu business worldwide.

They apply to both the personal data that we use to run our own business, for example data relating to our employees, as well as the data we process for our clients when delivering our commercial services.

Principle 1 - Accountability

Accountability is our first principle, because accountability is the strong foundation that ensures we do what we say and keeps us true to the 8 ways to the never before.

Accountability means continuing to invest in the right governance, people, processes, and systems across our business to objectively demonstrate to our stakeholders that we're acting with the honesty, integrity, and responsibility they demand – no matter where in the world we operate.

- ✓ **We will implement appropriate governance and assurance measures to ensure compliance with our data protection obligations and these principles.**

Principle 2 – Data Protection by Design

Data protection must be designed into the ways in which we collect, use, and manage personal data. It cannot be an afterthought, or simply a compliance box that needs to be ticked once a new product or process has been developed.

Getting data protection right means taking a human-centric approach, considering the issues related to personal data processing through the eyes of the individuals impacted, and being proactive in our thinking about how to manage risks.

- ✓ **We will systematically review how our collection and use of data may impact on individuals, and manage any risks identified responsibly.**

Principle 3 – Being fair and transparent

We believe responsible use of personal data has the power to generate value for individuals and businesses in the digital economy. Data collection and use must be fair, lawful, and transparent if we're collectively to build and maintain the trust required to make that opportunity real.

Individuals should be adequately informed about how their personal data may be collected and used and provided with ways to appropriately control this. In some cases, individuals may have legal rights over their personal data.

- ✓ **We will work closely with our clients and suppliers, where appropriate, to ensure clear information and choices related to personal data processing are provided to individuals at the right time.**

- ✓ **We will respect individuals' legal rights to control their data.**

- ✓ **We will only use personal data as permitted by data protection laws, and within any limits or constraints set out in any transparency notices or contracts with clients or suppliers.**

Principle 4 – Managing suppliers

We use trusted suppliers to help deliver our data driven services and assist us in running our business effectively and efficiently. We operate a risk-based framework to appropriately manage our supply chain, which includes undertaking due diligence where appropriate to reflect our commitment to the highest standards of integrity, ethics and responsible business practices. These commitments are made real by the requirements we impose on our suppliers which may require them to:

  - Promote awareness so they understand the importance of protecting personal data
  - Maintain robust security policies, standards, practices and controls to protect personal data
  - Use only personal data provided in accordance with instructions and law
  - Not use, disclose or otherwise process personal data provided by dentsu without first seeking approval
  - Only collect and process personal data necessary to fulfil agreed objectives, which must be relevant and not excessive
  - Not use any third party processor without appropriate security measures and data processing agreements being in place

- ✓ **We will responsibly handle our supply chain to proactively manage any data protection risks.**

Principle 5 – Data security

Keeping personal data safe and secure is essential to protecting people from any harm that would arise from a loss of confidentiality, integrity, or availability of their personal data.

- ✓ **We will have appropriate measures in place to prevent unauthorised use, access or accidental loss of personal data.**

Principle 6 – Purposes, data minimisation, retention and accuracy

Being clear about the purpose for which personal data is being collected and used is foundational to managing personal data well.

The principle of data minimisation means collecting only the minimum amount of personal data required for the purpose or purposes for which it was collected. When data is no longer required for those purposes, it should be erased or deidentified as appropriate.

In addition, personal data should be sufficiently accurate for the purpose(s) for which it is processed, taking into account the nature and context in which it is processed.

- ✓ **We will respect the principle of data minimisation**

- ✓ **We will work with clients and suppliers to ensure personal data is sufficiently accurate and up to date.**

August 2022: Issued.