Nestlé Good food, Good life

Nestlé's* Salient Issue Action Plan:

DATA PROTECTION AND PRIVACY

25 May 2022

nestle.com/sustainability/humanrights

EXECUTIVE SUMMARY

Definition of the issue

Data protection is about securing data against unauthorized access. Data privacy is concerned with the collection, storage and use of personal data and the rights of the individual whose information is being stored.

Why it matters

Data has enormous value, especially in our highly digitized society. It can help businesses to better engage with consumers, conduct innovative research and development, and deliver valued products. However, if not handled with care, it can lead to interference with people's private lives.

Geographical priority

Global

Key strategy and activities to address the risk

- The Nestlé Privacy Program and maturity self-assessment
- Privacy Impact Assessment as part of the privacy-by-design principle
- Compulsory Data Privacy iLearn module for relevant employees
- Vendor Privacy Risk Assessment as part of the due diligence
- Data Ethics as part of the *Nestlé Responsible Sourcing Standard*
- Regular internal and external audits

KPIs we will report on

- Number of data breaches annually

Value chain priority

* Nestlé throughout this document refers to the Nestlé Group

BACKGROUND

What we are talking about

Data protection is about securing data against unauthorized access.

Data privacy is concerned with the collection, storage and use of personal data and the rights of the individual whose information is being stored.

Why it matters

The digital age and technological advancements have made data a key asset for businesses. It can help organizations better engage with consumers, conduct innovative research and development, and deliver valued products. However, if not handled with care, it can lead to interference with people's private lives.

The law protects the fundamental right to privacy and provides people with greater autonomy over the way their data is collected and used. It also sets baseline standards for what companies can and cannot do with data.

There is a clear and growing trend for established data protection and privacy laws to be strengthened (such as the EU's GDPR), and for countries without laws to create new law. There is also a trend of greater consumer, investor, customer and regulator expectations in respect of privacy, data protection and how data is being used by corporations.

In addition, data ethics is becoming an area of increasing social and regulatory focus. Data ethics is about not only doing what is legal with data, but also what is right. In the digital age, where data and technology are inextricably linked, it is ethics rather than law that will guide us on how to use data. It is not only the "what" but the "how." Data ethics and ethical data management is critical in this emerging world of the digital economy.

Why this issue is relevant and important for us

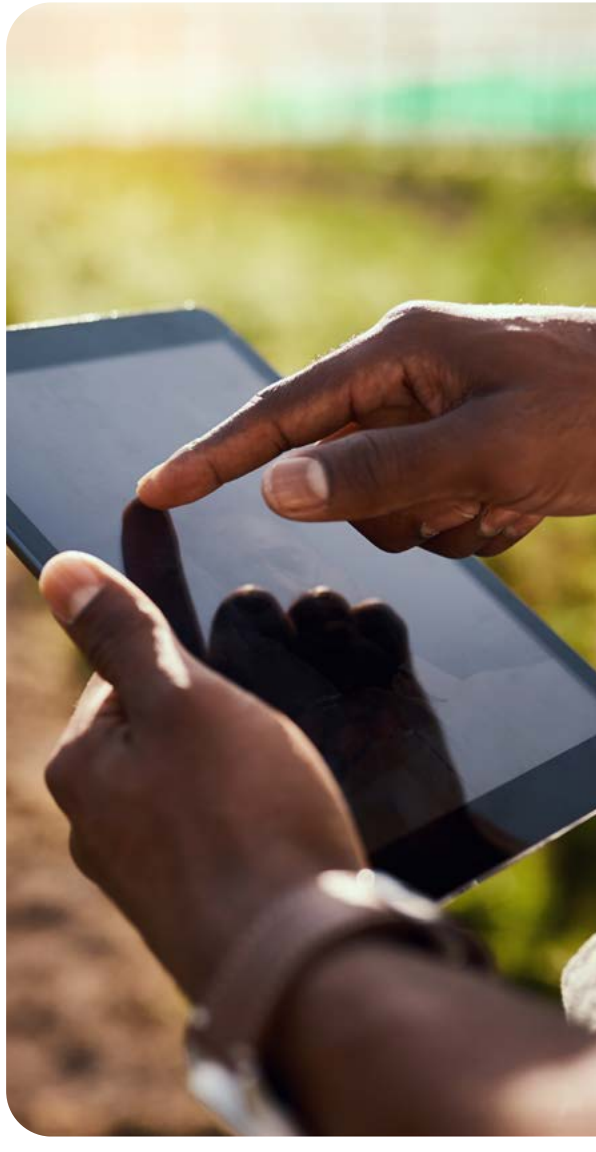
At Nestlé, our values are rooted in respect: respect for ourselves and respect for others, including respect for the privacy of individuals. This commitment to privacy is reflected in the *Corporate Business Principles*. Through this commitment, we, as Nestlé, strive to be trusted for our privacy practices and to succeed in the digital reality by living up to the changing expectations of our stakeholders.

With more data comes greater responsibility in protecting that data. Nestlé prides itself on being a company that is trusted by its consumers, employees and business partners. When our consumers trust us, they are likely to share more personal data with us, allowing us to know them better, and to deliver greater personalization and enhanced user experience. This is in line with our digital and e-business ambitions and reflected in the Nestlé Privacy Program, and applies to all Nestlé entities across the world, even if local law is more lenient.

The challenges in addressing this risk

Nestlé is a multinational company operating in almost all jurisdictions. This means we are subject to many laws and regulations, sometimes conflicting. This can make day-to-day working processes extraordinarily complex.

We believe that the most effective approach is to have privacy legislation that is based on internationally recognized data protection principles and promotes transparency in data use practices.



NESTLÉ'S VISION AND APPROACH

We avoid using data and technology in ways that are unethical or could lead to discrimination, exploitation or cause harm. We are committed to the ethical use of data based on the following principles: (i) Environmental and Social Wellbeing, (ii) Transparency, (iii) Diversity, Non-Discrimination and Fairness, (iv) Privacy and Security, (v) Accountability and (vi) Technical Robustness. Our commitment to data ethics is reflected in the *Nestlé Data Ethics Framework*.

We will continue playing our part in helping to protect the personal data of our consumers, employees and business partners through monitoring new data protection and privacy laws worldwide, collective actions and engagement with all relevant stakeholders to improve our standards.

Our vision and approach

As part of Nestlé's vision and ambition for data, we have made numerous commitments to process and protect the personal data of all our stakeholders in a compliant way. Our Privacy Program reinforces this commitment.

Nestlé is committed to respecting the rights of individuals in relation to their personal data. We recognize the right to privacy as a fundamental human right. We believe that maintaining the trust of our consumers, employees and business partners, and managing their data responsibly, are of critical importance.

The Nestlé Privacy Program ensures that privacy is embedded into our business operations and that the personal data we collect is processed lawfully and fairly, is kept secure against unauthorized processing, unlawful or accidental destruction, loss or misuse, and is deleted when it is no longer required.

We aim to prevent and address privacy issues wherever they occur within the Nestlé Group and our vendors. If we receive reports of data incidents, we investigate allegations and take action if there is evidence of wrongdoing.

We strive to be transparent with individuals in relation to how we process their data, and to provide them with meaningful control over how their personal data is collected and used, including responding to their requests and complaints.

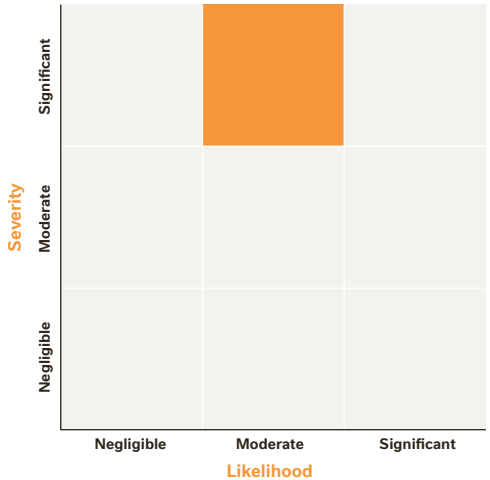
The Nestlé Privacy Program is the way we address the issue. It comprises:

- **Nestlé Privacy Policy** that defines a commitment to privacy and sets out key principles such as (i) privacy-by-design, (ii) processing for specific purposes, (iii) lawful, fair and transparent processing, (iv) properly managing personal data, (v) rights of individuals and (vi) security of personal data.
- **Nestlé Privacy Standard** that supplements the Nestlé Privacy Policy, reflects the Nestlé Group's commitment to respect privacy and sets out the data privacy standards for how personal data is processed by the Nestlé Group. It covers the personal data of Nestlé's consumers, employees and other individuals (e.g., individual employees of customers, suppliers and service providers).
- **Record Retention & Destruction Standard** applies to all records generated in the course of the operations of the Nestlé Group that we hold or have control over.
- The appointment of a **Group Data Protection Officer** and **Data Protection Champions** in the markets and businesses. Having the right people in place to address data protection and privacy matters is an integral part in protecting the employee, consumer and customer data of Nestlé.
- Compulsory **Data Privacy iLearn** module for relevant employees.
- Our vendors who process personal data are subject to the **Vendor Privacy Risk Assessment** as part of data privacy compliance and vendor management. It is important for Nestlé to ensure proper third-party management and vendor compliance with data protection standards.

In addition, all our suppliers must follow our *Responsible Sourcing Standard*, which sets out the requirements that we ask our suppliers to adhere to at all times when doing business with us, including data protection, confidentiality and privacy. We also incorporated a *Data Ethics Addendum* into the *Nestlé Responsible Sourcing Standard*.

2022–2025 ACTION PLAN

Assess: Our risk exposure



The "severity" of the issue on the heatmap represents the measures of a risk. It is linked to potential fines and corporate reputation. In the case of data privacy, the risk is significant. "Likelihood" represents the possibility of a risk to occur. Although we may have all data privacy controls in place, a potential data breach can happen.

In order to mitigate the risk, we use the following tools:

- Maturity self-assessment
- Privacy Impact Assessment as part of privacy-by-design principle
- Vendor Privacy Risk Assessment
- Internal and external audits

Address: Our priority actions

Nestlé: Taking action within our value chain

- Regular Vendor Privacy Risk Assessment as part of due diligence
- Close collaboration on data breaches with our vendors (if applicable), as well as local authorities
- Data breach procedure with internal security team includes root cause analysis of every data incident
- Training for employees on how to protect personal data and report potential data breaches

Collective action: Helping tackle root causes with all relevant stakeholders

Data breaches may happen due to cybersecurity threats or human errors in every company. We are committed to better understanding and helping tackle the root causes of this serious issue in close collaboration with internal security teams and vendors (if applicable), as well as local authorities.

We take an active role in the development of the regulations, policies and programs that are needed to make our vision a reality, including through industry associations we are part of:

- Center for Information Policy Leadership (CIPL) – a global privacy and data policy association working with industry leaders, regulatory authorities and policymakers to develop global solutions and best practices for privacy and responsible use of data to enable the modern information age.
- World Federation of Advertisers (WFA) – helps set standards for responsible marketing communications worldwide and encourages leadership initiatives that go beyond compliance with existing industry standards.
- International Association of Privacy Professionals (IAPP) – a not-for-profit association with an objective to provide a forum for privacy professionals to share best practices, track trends and advance privacy management issues.
- European Round Table for Industry (ERT) – advocates policies that underpin the values of freedom, tolerance, equality and openness.

Grievance mechanism

- If individuals are concerned about Nestlé's use of their personal data, they can contact the Nestlé Group Data Protection Office or local markets by using the contact details included in our privacy notice, which is available on all Nestlé websites.
- Concerns can also be raised via our Speak Up platform.

Monitor and report on KPIs, overall performance and challenges

Monitor

- Maturity self-assessments
- Internal and external audits

Report on KPIs

- Data breaches are reported in our annual *Creating Shared Value and Sustainability* report

We take an active role in the development of the regulations, policies and programs that are needed to make our vision a reality

GOVERNANCE FOR THIS ISSUE

Headquarter level

- Data protection and privacy matters are led by the Group Data Protection Office and Group Data Protection Officer, both in Group Legal and Compliance.
- The Nestlé Group Data Protection Office is supported by Data Protection Champions (DPC), who are the first point of contact within the markets/businesses/functions. The DPC and the Nestlé Group Data Protection Office together form the Nestlé Privacy Network (NPN).
- The Information Security Committee is the steering committee responsible for validating strategic privacy-related decisions.

Zone level

- Matters can be escalated to Zone Compliance Committees or Officers, and Management, as necessary.

Market level

- The Market Compliance Committees are responsible for ensuring compliance with the Nestlé Privacy Program at market level.
- Local Data Protection Champions are the first point of contact.

nestle.com/sustainability/humanrights