Data Protection Management System (DMS)
Henkel AG & Co. KGaA („Henkel Germany“)

Introductory Note

Henkel’s Data Protection Management System has been established in consideration of generally accepted frameworks and applicable legal requirements. Below, we describe the Henkel DMS as at October 29, 2019, as per the basic elements of a Data Protection Management System in accordance with IDW PS 980 and under due consideration of IDW PH 9.860.1. Henkel’s Data Protection Management System covers all management measures implemented at Henkel group companies to comply with applicable data protection laws (Data Protection), namely within the material and territorial scope of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).
The Management Board bears the overall responsibility for the Data Protection organization which is part of Henkel’s Compliance organization tasked with ensuring global compliance with laws and internal standards under the direction of the globally responsible General Counsel & Chief Compliance Officer (CCO).

1) Data Protection Culture

In an ever more digitized and data-driven economy, new data processing technologies bring about constant challenges to adequately protecting people’s privacy. Henkel’s strategy to become more customer-focused, more innovative, more agile and fully digitized in our internal processes and customer-facing activities naturally entails an increased amount of personal information in Henkel’s possession and used in more frequent scenarios.

Henkel’s ability to achieve its strategic ambitions depends on a positive relationship with our stakeholders (e.g. employees, consumers, business partners, suppliers, shareholders etc.). Any violation of applicable data protection laws is likely to damage Henkel’s reputation and may result in severe consequences for Henkel. Furthermore, such violations may possibly lead to civil or criminal risks for Henkel as well as any employee involved.

It is a core principle at Henkel expressed in Henkel’s Code of Conduct to operate in an ethical and legally correct manner. Compliance with applicable data protection laws is an integral part of such conduct. This is backed by the fundamental understanding that Compliance with applicable laws always takes priority over business goals if there is a conflict.

> ***“We recognize our obligation to respect the personal dignity and guard the privacy rights of all of our employees, customers, service providers and suppliers.”***
>
> *Code of Conduct*

Moreover, Henkel's internal EU Data Protection Policy conveys the fundamental understanding that all processing of personal data must be in compliance with applicable data protection laws, namely GDPR).

Henkel's Data Protection Culture is illustrated and summarized by the following statement of Henkel's CEO in the global Data Protection Compliance eLearning and reiterated at various occasions:

> ***"Data Protection is a critical factor in an increasingly digitalized world and the protection of personal data is and will be indispensable one of the top priorities within Henkel's compliance management strategy. It is in our all responsibility to ensure Data Protection compliance."***

The understanding that Data Protection is in everybody's responsibility has been reinforced by virtue of the "Commitment statement for the processing of personal data" rolled out to all employees worldwide.

2) Data Protection Objectives

Henkel is active in jurisdictions and countries, both strict and lenient with Data Protection regimes. Wherever Henkel operates, customers, partners, and employees have a legitimate expectation that the data entrusted to Henkel is kept safe and processed only for designated purposes. However, not all jurisdictions demand or even allow Data Protection according to a single global standard. Hence, Henkel's DMS focusses on data processing within the scope of the GDPR.

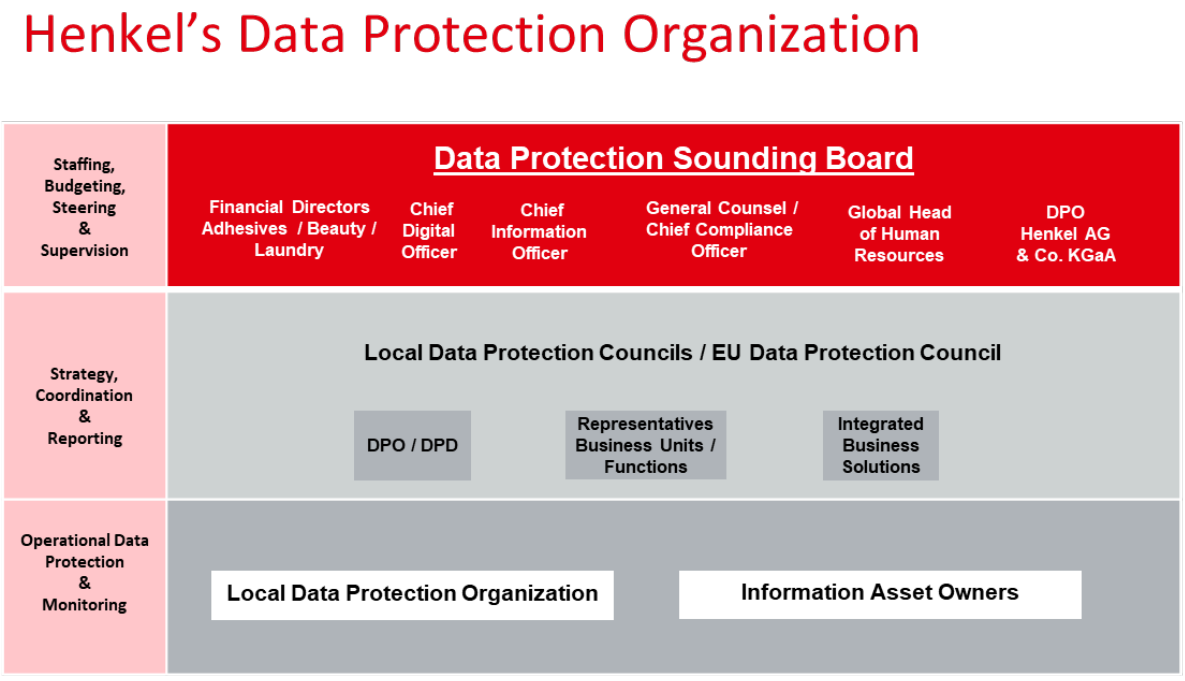
The DMS is valid for Henkel Germany and its affiliated companies within the territorial scope of the GDPR. It is laid out to implement the guiding principles derived from GDPR as defined in the Henkel's EU Data Protection Policy aiming at:

1. Implementation of a proper data protection organisation;
2. lawful processing of personal data;
3. necessary policies and standards;
4. workable compliance processes and procedures;
5. adequate data security measures; and
6. reliable mechanisms to prove compliance (accountability).

3) Data Protection Organization

Within the scope of the DMS, data protection compliance must be achieved on entity-level regarding all processing of personal data performed as a Controller or as a Processor (each an "Information Asset").

The **Management Board** bears the overall responsibility for ensuring compliance with applicable laws and internal standards globally. Henkel has established an interdisciplinary **Data Protection Sounding Board**, chaired by the DPO of Henkel Germany, to provide for the staffing and budgeting, and to steer and supervise the Data Protection Organization across the scope of the DMS.



Each Henkel entity within the scope of the DMS which is Controller and/or Processor of Information Assets shall appoint a **Data Protection Officer** (DPO) or **Data Protection Delegate** (DPD) with the same tasks as defined for Data Protection Officers in the GDPR, and, in particular to keep an inventory of all Information Assets containing personal information as notified in the relevant processes, and to serve as point of contact for 3rd party requests.

Each DPO / DPD also chairs the **Data Protection Council** implemented for the respective entity, consisting of appointed delegates from each Business Unit active in the respective entity, HR, IBS as well as other suitable persons appointed by the DPO / DPD. The Data Protection Council is entrusted

with tasks regarding strategy, coordination and reporting, in particular evaluating data protection-related processes and policies, monitoring the implementation of data protection-related actions, and reporting the status of the entity to the local management which, in the case of Henkel Germany, is represented by the Data Protection Sounding Board.

The **European Data Protection Council** consisting of all DPOs / DPDs and chaired by the DPO of Henkel Germany has been implemented for the biannual consultation between Henkel entities, in particular regarding issue of internal data transfers, Controller-Processor relationships and other topics regarding more than one entity or group of countries with shared management functions.

Operational data protection (e.g. ensuring lawful processing, processor management, compliance with internal data protection management processes, monitoring (1st line of defense), maintaining appropriate documentation to demonstrate compliance with the GDPR etc.) is the task of the **Information Asset Owners**. Information Asset Owners must have sufficient know-how and the necessary resources to fulfil their tasks as well as authority to change or stop data processing activities.

The Corporate IT Organization (IBS) is responsible to define technical and organizational measures in line with GDPR and other relevant jurisdictions, to implement processes ensuring that any introduction or change of an Information Asset respect the principles of data protection by design and by default, as well as to monitor the conformity with such corporate policies on a regular basis. Also, IBS nominates and renders data protection support for each country in scope of the DMS.

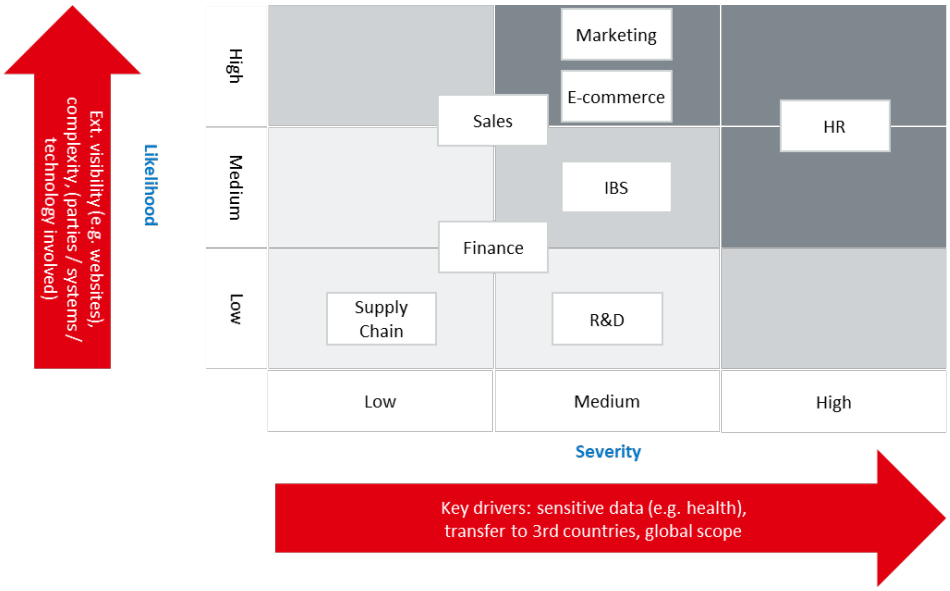
Roles in Henkel's Data Protection Organization

Asset Owners	DPO	IBS
Lawful processing	Inform & advise	Define TOMs
Comply with internal rules	Documentation Hub	IT Demand process
Monitoring & Documentation	Monitor compliance	Privacy by Design
	Point of contact for externals	Support DPO + Asset Owners

4) Data Protection Risks

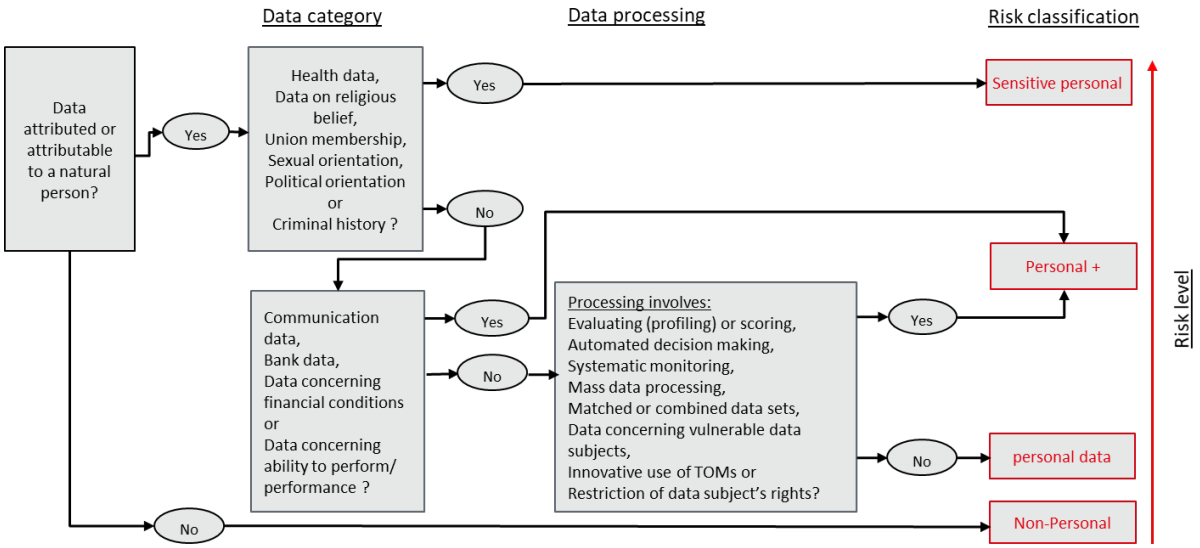
Data Protection Risks need to be assessed from the point of view of the data subjects (the persons concerned by data processing). Hence, the severity of risks is embodied mainly in the type of data which is processed and the means of processing whereas the likelihood of a risk is predominantly driven by the exposure and the complexity of the processing. At a high level, this view results in a risk matrix for Henkel which identifies the presence of consumer or HR data and the degree of digitalization of a certain area as the main risk drivers (**top-down-approach**).

Risk matrix for Personal Data Processing @Henkel



The risk present in any given Information Asset (**bottom-up-approach**) which is also used for the purposes of the risk classification according to Henkel's IT Security System is assessed in a separate methodology factoring data types as well as certain types of processing. It can be used to determine whether processing of personal data represents a risk which is solely created by the fact that personal data is processed ("personal"), special categories of personal data according to GDPR are processed ("sensitive personal"), or certain defined data categories and risk drivers point towards an elevated risk embodied in the processing in the Information Asset ("personal+"). **Data Protection Impact Assessments** are used to assess and remedy any high risk present in Henkel's processing of personal data.

Risk classification



5) Data Protection Program

Henkel's DMS is based on **globally binding Corporate Standards** and, where necessary, complementing policies. The core piece of the DMS is the EU Data Protection Policy detailing Henkel's implementation of all GDPR-compliance related measures. It relies on a strong IT security governance as implemented by Corporate Standard Information Security which has been adjusted to fit the additional needs spelled out by GDPR. Both may be accompanied by additional policies put in force for certain countries or areas of business to support and ensure GDPR-compliance, namely a Data Breach Management Policy which sets out a framework for the effective identification, internal management and external notification of **data breaches.**

For each Henkel entity which is Controller and/or Processor of Information Assets, the respective DPO / DPD keeps an inventory of all relevant Information Assets (presenting a Record of Processing Activities) as well as a process to reflect change and ensure content as appropriate. Henkel employs state-of-the-art **IT tools** for the administration of data protection related management tasks.

Compliant processing needs to be achieved per Information Asset. Information Asset Owners safeguard **lawful processing**, i.e. they ensure that either a valid legal provision or the demonstrable consent of the affected individuals allows the use of data relating to an individual and that all other relevant principles of lawful data processing are observed at all times.

This entails ensuring implementation of appropriate **technical and organisational measures** to protect personal data, including protection against unauthorised, unlawful processing or change of purpose and against accidental loss, destruction or damage as well as ensuring duly and timely **deletion**, taking into account the state of the art (including continuous changes and projects) and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects. The standard of technical and organisational measures of data protection applied at Henkel is described in the Corporate Standard Information Security and complemented by specific stipulations, e.g. stemming from DPIAs.

Moreover, the Information Asset Owners provide **transparent** information about the processing to the **data subjects** allowing them to effectively assert their rights granted by Law. The DPO / DPD as designated point a of contact for externals assists with establishing an effective internal complaint-handling mechanism.

Asset Owners notify introduction and replacement of a **Processor** to the DPO/DPD. Processors are regularly checked for their ability to provide services according to Henkel's standards and for appropriate technical and organizational measures; checks are performed by surveys, audits or other suitable measures. The DPO / DPD keeps an overview of all Processors employed by the respective entity.

In case processing entails any **data transfers to a Third Country,** Asset Owners notify such data transfers; appropriate safeguards and availability and enforceability of data subject rights and effective legal remedies are verified regularly.

As a highly international corporation Henkel relies on internal international data transfers to make data available to the appropriate managers in the Group's matrix organization. Henkel has defined a corporate data transfer governance for Information Assets transferring Personal Data to Henkel entities in Third Countries; standard contractual clauses are in place between the relevant Henkel companies to provide appropriate safeguards, enforceable data subject rights and effective legal remedies for data subjects.

Data breaches detected through audit, monitoring or otherwise have to be reported to the respective DPO / DPD by the means and in the form defined in the Data Breach Policy without undue delay; a 24h hotline is in place to collect notifications outside regular business hours. The DPO /DPD determines whether a notification to the data protection authorities and/or the persons concerned by the data breach is necessary and, if so, issues such notification.

6) Data Protection Communication

Communication on data protection is disseminated broadly, ranging from general information on the intranet, on sharepoints, in mass mailings or other channels accessible to all employees or addressing certain parts of the company to target-oriented detailed information aimed at individual stakeholders and discussions with corporate bodies.

Data protection processes and standards are communicated to Henkel's employees at multiple levels. **Training** and communication measures are tailored to the risk profile of Henkel's businesses and the stakeholders' activities. This includes voluntary and mandatory eLearnings and face-to-face trainings to Henkel's employees as well as guidance to new employees by means of the employee on-boarding process. Further enhancement of the data protection training program, particularly with regard to trainings for Information Asset Owner and other internal stakeholders determined by a risk-based approach (e.g. HR, IBS and consumer data related marketing), is a key priority for Henkel's data protection organization.

All employees can solicit proper advice on data protection issues. They are encouraged to contact the respective DPO / DPD, the Henkel Law Group or the respective Information Asset Owner at any time.

Reporting on data protection is regularly provided by the DPO / DPD to the management bodies of the respective entity (in the case of Henkel Germany to the Data Protection Sounding Board) and, in cases of material issues or to obtain resources or decisions, to the Data Protection Sounding Board. All DPOs / DPDs contribute to the annual data protection-reporting issued by the local Presidents to Henkel's Compliance Organization and then compiled for Henkel's Management Board. Additionally, the DPO of Henkel Germany issues an annual DPO-report to the management bodies of Henkel Germany.

7) Data Protection Monitoring and Improvement

Henkel's data protection efforts are constantly **monitored** by Henkel's management: by responsible management bodies and the Data Protection Sounding Board, by the Information Asset Owners regarding the appropriateness and effectiveness of data protection measures for their respective Information Asset, and by regular internal checks and audits performed by Corporate Audit and the DPO / DPD verifying effectiveness of the DMS. The data protection organization collaborates with Corporate Audit, which plans and performs the vast majority of internal audits at Henkel, according to an audit plan derived from a risk-based audit approach. Country audits are regularly conducted in selected countries by the data protection organization, often with the support of external law firms.

Data protection matters are regularly discussed with Henkel's external legal advisors. Henkel's data protection approach is aligned with external legal counsel which regularly advises on further **improvements** and new regulatory requirements.

The data protection organization actively networks in external compliance forums which allows the exchange of know-how and **benchmarking** with peers. **Best practices** are identified, implemented, and lead to improvements in Henkel's data protection processes. **The identification of control weaknesses** and the implementation of appropriate remedial measures (e.g. during the remediation of a data breach) is part of Henkel's data protection reporting, including development of major compliance initiatives which are rolled out across several affected entities.

Continuous improvement of the Compliance organization reaffirms Henkel's ambition to meet the highest standards in operating its data processing activities in an ethical and legally correct manner.

Düsseldorf, October 29, 2019

Henkel AG & Co. KGaA