Description of the METRO

Data Protection Management System

Data Protection Culture

Data Protection Mission

1. The METRO AG Board of Directors has organizational and supervisory responsibility for data protection matters. The Corporate Data Protection Department ("DPD") as implemented a risk-based Data Protection Management System ("DMS") in order to fulfill these responsibilities.

2. The principal component of the DMS is METRO's General Data Protection Guideline ("Data Protection Guideline") which, among other things, creates and organizational framework for data protection within the METRO group of companies ("METRO") and specifies more detailed responsibilities in the area of data protection. These specify certain criteria for the creation and operation of an appropriate compliance organization with regard to the handling of data protection questions.

Creation of Data Protection Awareness

3. METRO believes that a sustained and positive data protection culture is necessary for an effective DMS. The data protection culture at METRO is expressed in the manner in which individual METRO employees handle personal data, protect it and how they make the handling and/or protection of such data transparent from the outset.

4. Data protection culture concerns all functional areas. A positive data protection culture starts from top management: at the METRO managing director level. Managers are responsible for being role models by promoting compliance with data protection related laws and regulations. In this regard, METRO places responsibility on managers and directors. However, this applies likewise to all managerial staff at the director level both in the main offices and in the markets.

5. The most important cornerstones of the METRO data protection culture relate to protecting the privacy of our employees, customers and business partners. METRO is aware that the protection of fundamental rights is an essential component of our corporate culture and that compliance with these standards directly influences perception as an attractive employer as well as our internal and external reputation. METRO is also aware that compliance with data protection requirements represents an essential component of the overall Group compliance strategy and an important factor in preventing reputational damage and other associated risks for METRO and its brands. The Board of Directors communicates with employees con-

cerning data protection issues on the Intranet, anchors protection of privacy as an essential component of developing the corporate culture and emphasizes the special responsibility borne by the company in this regard.

6. METRO intends to employ technical innovations on a continuous basis for the benefit of the Group, its employees and customers. As part of the digitization strategy, METRO intends to optimize the value chain for personal data, streamline the data flow within the Group and create innovative digital business models. Ensuring the utility of existing and new data portfolios is thus an essential prerequisite for the Group's future business strategy, which in turn may only be achieved subject to strict compliance with data protection related requirements.

7. METRO sees every business process associated with the processing of personal data (processing activities) as an opportunity to obtain a better understanding of the customers, to continue to improve the company's collaboration and performance and to discover and exploit new market opportunities.

8. Employee compliance with official guidelines regarding data protection is evaluated as part of the regular METRO employee evaluation process. Any breaches of data protection guidelines are addressed as part of this process and reflected in the regular evaluations.

Data Protection Objectives

Definition of Data Protection Compliance

1. The objective of DMS is to manage the company in compliance with applicable laws and internal policies that affect relevant data protection risk areas.

2. The DMS is a component of the company's overall compliance strategy to ensure that it acts lawfully. The DMS provides support to the company in complying with legal and statutory requirements in the field of data protection and thus aiding METRO in avoiding administrative measures - in particular fines and penalties - as well as civil law claims and reputational damage.

3. In this context, the cornerstones are provided by binding national laws and regulations related to data protection (the Federal Data Protection Act in Germany as well as other data protection specific laws, regulations and statutes) and the General Data Protection Regulation for the European Union 2016/679 ("GDPR") within the European Union. In addition, the Data Protection Guideline is binding internally within the entire company to the extent not otherwise provided therein.

DMS Concept

4. Applicable legislation and regulations are to be reviewed on a continuous basis by the data protection officer for their currency and to undertake any necessary changes or additions. In addition, statements from competent authorities and

court rulings must be noted and reviewed. Any needed changes determined on the basis of this review flow into the DMS and internal data protection policies.

5. Accordingly, each instance of personal processing must be examined as to whether it conforms to applicable laws and the Data Protection Guideline. As part of this process, the first step is to clarify the underlying facts and to examine them in light of the standards set by the relevant requirements. Data protection related risks should be weighed against any business related pros and cons in all cases should any doubts or risks remain following a complete review.

DMS Scope of Application

6. The DMS applies to all members of the METRO group of companies on a global basis ("METRO Companies"). However, more stringent requirements apply to the processing of personal data within the scope of the GDPR; these are expressly specified in the Data Protection Guideline.

7. All business areas and processes within a METRO Company fall within the scope of the DMS. There are no simplified or reduced requirements for "minor" processes, for example if data is only processed to a limited extent (small number of data subjects). As soon as a process involves the processing of personal data it must comply with the requirements of the DMS. Only those processes that do not involve the processing of personal data at all fall outside of the scope of the DMS.

8. Similarly, the DMS applies to all types of personal data, regardless of whether this involves personal data from customers, suppliers, employees or other data subjects. In this regard employees are unusual in that they process personal data and, at the same time, may be affected by data processing.

Data Protection Objectives

9. Data protection objectives include both compliance with binding data protection requirements and applicable law as well as the intent to present METRO as a reliable partner for customers and business partners along with its own employees. An additional objective is to use personal data for new business strategies subject to compliance with data protection rules and regulations.

10. In addition to the Data Protection Guideline, the objectives of the DMS are communicated via handouts and generally accessible information pages on the Intranet. They are also part of the METRO non-financial statement ("NFS").

11. Achievement of data protection objectives is detailed in annual data protection reports for each company prepared by the respective data protection officers at the companies which is then presented to the boards of directors.

Data Protection Organization

Structural and Process Organization

1. The data protection organization at METRO is designed for structural and operational efficiency. A variety of roles have been defined within the data protection organization.

2. The boards of directors of the various METRO Companies are obliged to define and implement all measures required in order to ensure compliance with applicable data protection laws and regulations by their respective companies. The boards of directors are responsible for compliance with applicable data protection laws and regulations within the companies. The implement guidelines at the management level in the area of data protection subject to consideration of any applicable legal variances based on applicable national laws. Accordingly, company group management is subject to support and monitoring obligations. Managing directors of METRO Companies provide the required personnel, organizational and financial resources within their companies in order to ensure an appropriate level of data protection within the relevant legal framework.

3. Each METRO Company is required to appoint a data protection officer subject to the requirements of Annex 2 to the Data Protection Guideline - even in cases where this would not be legally required. The data protection officer satisfies all tasks and duties for which they are responsible under applicable local law and Annex 2 to the Data Protection Guideline at the respective METRO Company as relates to data protection related matters, including without limitation (a.) advising METRO Companies in data protection related matters, (b.) supporting METRO Companies in compliance with applicable data protection laws, the Data Protection Guideline and other binding internal guidelines from METRO related to data protection and (c.) monitoring all of these requirements.

4. Each data protection officer is expected to work closely with the respective company management board. Each data protection officer reports directly to the board of directors and closely coordinates data protection issues with the board, e.g. as part of regular meetings with the managing director responsible for data protection matters.

5. As the central data protection unit, the task of the DPD is to provide support to the METRO Companies and their data protection officers in matters related to data protection and to revise and update existing data protection rules and policies.

6. In addition to conceptual DMS responsibility, the DPD supports all METRO Companies and their data protection officers in implementing DMS measures. In addition, DPD offers a large selection of practical aids, templates and information related to application in day-to-day practice.

7. At least two data protection managers work within the DPD who are responsible for top-level data protection matters within METRO. Among other things, the data protection managers assume the tasks (a.) advising data protection officers in da-

ta protection related matters, (b.) coordination of data protection questions related to Group issues, (c.) monitoring the data protection officers and (d.) preparing regular reports concerning the general status of data protection at METRO. Data protection managers are authorized to request information about all processes and circumstances related to the handling of personal data from all METRO Companies. They report directly to the METRO AG Board of Directors.

8. Each METRO Company must name at least one data protection coordinator. In the event the data protection officer believes it to be necessary, additional data protection coordinators in a reasonable number are to be named at their suggestion with the mutual agreement of the management of the respective METRO Company. The primary tasks of the data protection coordinators is to provide support to the data protection officer and company management related to compliance with applicable data protection laws, including the Data Protection Guideline and other binding internal requirements imposed by METRO in the area of data protection.

9. Responsibility for the overall data protection related conformity of business processes in relation to company management is retained by the process owner, i.e. the person with operational responsibility for the business process concerned. The process owner may coordinate with the data protection officer and the data protection coordinators and request their assistance in this context. They are responsible for maintaining and updating the record of processing activities.

10. The system owner is responsible for providing support when implementing data protection requirements in the IT system, in particular collaboration with the implementation of deletion concepts or complying with the requirements concerning "Privacy by Design" and "Privacy be Default." The system owner is the person responsible for the respective IT system used for processing personal data.

11. There are centrally defined qualifications for these roles within the data protection organization contained in Annex 2 to the Data Protection Guideline. They must be satisfied in order to hold one of these roles.

Data Protection Officer

12. A data protection officer must be appointed within every METRO Company provided that this is required based on the criteria specified in Annex 2 to this Data Protection Guideline. Only persons who satisfy the requirements set out in the job description contained in Annex 2 of this Data Protection Guideline may be appointed as data protection officers. Without limitation, it must be ensured that such person has the relevant qualifications needed to fulfill the role of data protection officer. In the event of any updates to the job description, the respective METRO Company must examine whether the data protection officer continues to fulfill the requirements.

13. Each METRO Company ensures that the data protection officer is able to fulfill the obligations incumbent upon then as defined in Annex 2 to the Data Protection Guideline and that they are able to exercise their authority. Without limitation, the data protection officer is to be afforded access to personal data and processing activities. METRO Companies are to ensure the independence and autonomy of the

data protection officer. The data protection officer must be involved in decision making and information processes at an early stage.

14. The contact information for the data protection officer is to be communicated within the company as well as externally and provided to the competent supervisory authorities.

15. The data protection manager provides advice and support to the data protection officer concerning the implementation of measures that ensure compliance with applicable data protection rules and regulations. In addition, the data protection officer is authorized to consult the legal department at the relevant METRO Company regarding legal questions affecting and related to data protection matters and/or may obtain external legal advisory services.

16. Transnational and uniform advisory services for the METRO Companies are ensured via the relevant data protection manager.

17. The data protection officer, as well as employees tasked with assisting the data protection officer in fulfilling their duties, must be verifiably obliged to maintain confidentiality.

18. The data protection officer is responsible for collaboration and coordination of data protection related matters arising in the METRO Companies in relation to authorities and data subjects.

Integration of the Data Protection Function and Interfaces to Additional Government Functions

19. Departments and functions within the relevant METRO Companies dealing with data protection related tasks communicate with a variety of other functions within their own company for purposes of technical consultation and coordination needs. Specifically, this includes the following departments: Compliance, Information Security, Internal Audit, Employee Representatives and the Legal Department. Regular, mutual communications are required between the individual departments and the data protection officer.

Risks

Data Protection Related Risk Management

1. The METRO DMS deals with a variety of risk areas that are based on the respective requirements under data protection laws. Without limitation, this includes documentation and accountability obligations, generally applicable legal principles governing data protection, deletion requirements, rights of data subjects and the security of data processing.

2. As part of the global DMS, data protection related risks are addressed by defining specific structural and operational measures and such measures are then per-

formed and/or monitored by the METRO Company data protection officers. The data protection manager within DPD defines such measures. The intent of these measures is to satisfy the minimum requirements. Each METRO Company, in particular the country management level and the relevant data protection officer are required to consider whether additional measures are required in order to adequately address data protection risks.

3. The implementation of these measures, as well as additional key indicators for each METRO Company, are monitored using a Data Protection Maturity Matrix. The Maturity Matrix calculates a "maturity score." The highest possible score is 100% and the score reflects the data protection maturity level for the respective METRO Company.

4. Measures will need to be revised to the extent that local legislation requires a stricter approach.

5. Every METRO Company conducts an annual assessment of data protection risks using testing criteria as part of the group-wide risk inventory conducted by METRO AG. As part of this process, data protection risks are to be updated as needed and new data protection risks must be included. These are assessed with the participation of the data protection officer.

6. Process owners conduct risk assessments relate to processing activities in order to identify potential new data protection risks and - if necessary - re-classify existing data protection risks. The frequency of these analyses depends on the assessment of the data protection risk concerned. Risk assessments related to processing activities with high or very high data protection risks are conducted annually provided that more frequent reviews are required according to administrative regulations or court decisions.

7. Risk assessments consist of bilateral meetings or a workshop format with the relevant staff member from the IT department and the data protection officer for the respective company in each case. The data protection manager is to be informed in the case of intra-group processing activities and must be included on a case-by-case basis.

8. The risk assessment must include the following elements regardless of the selected format:

    - Risk identification on the basis of risk scenarios that include, for example, different forms of data protection risks;

    - Risk assessment on the basis of potential damage and probability of occurrence (formula = damage amount x probability of occurrence = risk).

    - Risk classification: amount of damage and probability of occurrence are to be divided into four levels (classifications): "low," "medium," "high," and "very high." The following criteria are to be used as the basis for the risk classification process: a) assessment/scoring (including profiling); b) auto-

mated decision making with legal or other equivalent consequences; c) systematic monitoring and control; confidential data or highly sensitive personal data; d) large-scale data processing; e) reconciliation or aggregation of large data sets; f) data related to vulnerable data subjects; g) innovative use or application of new technological or organizational solutions; h) data transfers outside of the European Union; i) anything that prevents a data subject from exercising a right or the use of a service and/or the performance of a contract.

- Risk management in order to deal appropriately with existing risks and risks newly identified during the assessment.

9. Data protection risks must be documented in the record of processing activities for each processing activity and, to the extent necessary, communicated to the respective management level at the time a risk is identified in the case of high and very high data protection risks. In addition, data protection officer is required to monitor and document the processing activity in a manner appropriate to the data protection risk.

10. The DPD communicates specialized knowledge to the data protection officer in particular and to the operational departments involved in data protection. This relates specifically to the methods for correctly performing a risk assessment and that conforms to METRO risk management requirements.

Data Protection Impact Assessment (DPIA)

11. Processing personal data may represent an increased risk for the rights of data subjects as relates to their privacy and data protection. In the case of increased risk, the process owner for the respective METRO Company performs a preliminary risk assessment pursuant to Article 35 GDPR.

12. The document "Data protection impact assessment," which is available on the Intranet, is to be used for purposes of performing the data protection impact assessment. This reflects the applicable statutory rules, for example, the obligation to report to authorities. In particular, the data protection impact assessment is intended to include risk sources and scenarios, probabilities of occurrence and the amount of any damages. The process description contained in such document is binding. Documentation is to be prepared within the record of processing activities.

13. The necessity test and the data protection impact assessment are to be conducted by the process owner with the assistance of the data protection coordinator and, if needed, the data protection officer.

Data Protection Program

Data Protection Policies

1. The data protection rules and policies consist first and foremost of the Data Protection Guideline, its Annexes and the specific work instructions referred to therein. The Data Protection Guideline was adopted by the Metro AG Board of Directors. In addition, further rules are listed in specific policies and guidelines. They are binding by virtue of general references in the Data Protection Guideline. The complete body of rules and policies may be accessed via the Intranet. The Data Protection Guideline was sent to the persons designated as responsible in the Group Guideline "Principles of Rule Management."

2. New rules and changes to the existing rules will be communicated to the relevant manager. A Group Guideline, "Principles of Rule Management", that contains relevant rules in place in order to ensure the communication, topicality and binding nature of the rules within METRO Companies. Based on this guideline, the METRO Companies are obliged to adopt these rules as binding instructions within the relevant company subject to the requirements of applicable local law.

3. The rules must also be offered by the METRO Companies in the relevant local language in order to aid in comprehension.

4. The Board of Directors is required to apply a periodic-cyclical optimization process (Plan-Do-Check-Act) in order to ensure that Data Protection Management is updated to reflect legal, organizational and technical changes affecting the processing of personal data; all such updated must be risk-based and comply with applicable legal requirements. The data protection rules und policies are updated and revised by the DPD as part of this process so that they comply with current legal requirements. This is one of the core tasks of the DPD.

Record of Processing Activities

5. Every METRO Company is required to maintain a record of processing activities and to update it regularly. All processing activities that include the processing of personal data must be included in this record. The relevant process owner is responsible for the inclusion and maintenance of a process. The data protection coordinator for the respective business division provides support to ensure that all process owners within a business division record the processes for which they are responsible.

6. According to the Data Protection Guideline, the obligation to maintain a record of processing activities applies even if no such obligation is legally imposed on the respective METRO Company. By contrast, if the maintenance of a record of processing activities is legally required, the statutory provisions regarding the manner in which the record of processing activities is to be maintained have priority over the provisions of the Data Protection Guideline in the case of any variations.

7. Special rules for the maintenance of a record of processing activities apply within areas covered by the GDPR; they are specified in Annex 1 to the Data Protection Guideline. Their purpose is to implement the provisions of Article 30 GDPR.

8. Processes are recorded with the aid of software - currently the "PrIME" software application. Every process owner is provided a web-based questionnaire by data protection officer of the respective company in which they can enter all information relevant to the process. The responses are automatically transferred to "PrIME."

9. The process owners are provided support in completing the questionnaires in the form of sample questionnaires and instructions (tutorials). In addition, they can contact the data protection coordinator and/or the data protection officer. Additional materials are also available to the process owners as support aids. For processing based on consent, the DPD provides, for instance, a model consent form on the Intranet in addition to the requirements set out in the Data Protection Guideline that includes the required elements of an effective consent including required wording and (placeholder) contact information for purposes of withdrawal.

10. The information provided in the record of processing activities must be updated on an ad hoc basis in the event of changes to the processing activity. For example, an ad hoc change may be required if the purpose of the processing changes. Whether and when this may be the case is set out in a work instruction published on the Intranet addressing how to handle changes in processing purpose. Otherwise, the data protection officer requests the process owners to review the process on a regular basis (currently annually) by sending them questionnaires concerning existing processes for review.

11. Each data protection officer has access to the record of processing activities for the company for which they have been appointed and monitors the completeness and currency of the record of processing activities. As part of this review, they examine the respective processing activity including with regard to the lawfulness of processing.

12. The relevant data protection managers national/international have access to processes at all companies for which they provide support.

Technical and Organizational Measures

13. Each METRO Company is required to implement necessary technical and organizational measures ("TOM") in order to protect personal data.

14. The necessity of technical and organizational measures is based on a risk-focused assessment. In this context, this should assess, without limitation, the purposes of the processing, the probability of occurrence and seriousness of the risks for the rights and freedoms of data subjects on the basis of the current state of the art, the scope and circumstances of the processing, as well as the costs of implementation for any technical and organizational measures.

15. All IT systems in use by METRO are documented in an online tool. The function of the respective IT system is described there. In addition, a responsible person is named who may be contacted for questions about IT systems.

16. Each process owner is obliged to implement required technical and organizational measures for processing activities for which they are responsible and to describe them in the record of processing activities. Technical and organizational measures for specific processes are considered and implemented in collaboration between the process owners, system owners and data protection officers.

17. There is a METRO TOM standard catalog available for in-house METRO processing activities which describes standard technical and organizational measures that are in place for all processes included in the METRO IT infrastructure.

18. The METRO TOM standard catalog is based on the internal METRO IT Security Guideline which includes a comprehensive and detailed description of IT security measures within the company. The IT Security department is responsible for this Guideline and updated on a regular basis (annually for IT Security Management Principles, the Guideline is updated at scheduled intervals or as needed). Updates to the Guideline are then discussed between the IT Security department and the DPD with regard to their implications related to data protection and, as needed, included in the METRO TOM standard catalog. A new version of the METRO TOM standard catalog is approved jointly by the IT Security department and the DPD and is included as adopted in the record of processing activities as a TOM standard catalog after IT Security and the DPD have concluded that the measures are appropriate and effective.

Privacy by Design and Privacy by Default

19. The data protection principles of "Privacy by Design" and "Privacy by Default" are applied in particular when considering and implementing technical and organizational measures. Comprehensive rules on this topic are contained in Annex 4 to the Data Protection Guideline specifying appropriate business processes in order to ensure that these principles are followed. Without limitation, these rules apply to the new development and enhancement of existing IT systems and/or applications.

Rights of Data Subjects and Information Requirements

20. Data subjects affected by the processing of personal data by METRO must be informed of the processing of their personal data in harmony with applicable legal requirements. As a rule, personal data should be collected directly from the data subject themselves. Data collection from third parties pursuant to the Data Protection Guideline requires a legal basis.

21. Every data subject must, at a minimum, be informed of the identity of the METRO Company collecting data, the processing purpose as well as any additional recipients of their data and their rights in relation to such processing. Special requirements apply within the scope of the GDPR with regard to transparent information to be provided to data subjects as indicated in particular in Articles 12 to 14

GDPR. The process owner is responsible for ensuring compliance with these information obligations. If needed, they can request assistance from the data protection coordinator and the data protection officer. In addition, the data protection officer has provided a sample document to be used for providing mandatory information that includes instructions regarding the format in which information is to be provided.

22. METRO responds to inquiries from data subjects with regard to the rights to which they are entitled (access, rectification, erasure, restriction of processing, data portability and objection) without undue delay and no later than one month after receipt.

23. A model process described in a work instruction available on the Intranet as well as in a guideline (data portability) is in place for how data subject inquiries are to be handled internally. This provides detailed instructions on the steps to be taken following receipt of an inquiry until it has been answered and which departments within the company are required to take which sub-steps.

24. Steps must be taken to ensure that the identity of the data subject has been verified when responding to an inquiry from a data subject. For this purpose, METRO provides a model process for all companies for the identification of data subjects that must be implemented taking applicable local law into account.

25. In addition, sample answers are provided on the Intranet that are to be used when responding to inquiries.

26. The use of personal data for fully-automated decision making (e.g. scoring) is not permitted unless a legally-defined exception applies.

27. The treatment of data subject rights and handling of information obligations are subject to continuous review by the data protection officer. The guidelines are revised accordingly in the event of statutory changes or decisions by data protection authorities and/or courts.

Deletion Concept

28. A deletion concept is to be created and implemented by the process owner for each processing activity prior to the start of such activity.

29. The following must be ensured via the implementation of appropriate measures:

    - Documentation of deletion and blockage deadlines as well as blocks in the record of processing activities;

    - Organization of responsibilities with regard to the deletion and blockage concept;

    - Regular, at least annual, random sampling review of the deletion and blockage concept;

- Logging and monitoring of deletion/blockage.

30. Details regarding the organization and implementation of a deletion concept as an essential component of the DMS are specified in a binding manner in Annex 2 of the Data Protection Guideline.

Notification Process, Personal Data Breaches and Whistleblower System

31. Personal data breaches may result in a risk to the rights and freedoms of data subjects and must therefore be identified immediately so as to facilitate prompt resolution and timely reports to the supervisory authorities and data subjects pursuant to Articles 33 and 34 GDPR.

32. All METRO employees are obliged to report personal data breaches as soon as they become aware of them even if it is only a suspected personal data breach. Personal data breaches reported to employees by others (data processors, third parties) must also be reported. Employees are informed of this at training courses as well as fliers and information on the Intranet. All employees have access to information for identifying and reporting incidents on the Intranet.

33. Reports may be sent by e-mail to the official in-box of the data protection officer, or by telephone or in person. Employees may also report personal data breaches to data protection coordinators and data protection managers. They are obliged to forward the report to the relevant data protection officer at the applicable METRO Company/ies without undue delay.

34. Data processors are contractually obliged to report personal data breaches to the data protection officer at the relevant METRO Company without delay. All data processing agreements concluded by METRO include a reference to the official in-box for the relevant data protection officer to whom a report is to be sent.

35. Third parties may submit a report at any time using the official in-box for the data protection officer. This is to be included in all information for data subjects pursuant to Articles 13 and 14 GDPR.

36. Forms are available to employees and data protection officers at METRO for purposes of reporting personal data breaches. These forms simplify the collection of all required information concerning the personal data breach concerned.

37. The data protection officer is responsible for aggregating all information required for investigating the personal data breach, the resulting risk for the rights and freedoms of data subjects and the assessment of risk-mitigation measures that have been or are to be undertaken and to perform a risk assessment.

38. The data protection officer is required to involve the relevant operational departments when investigating and resolving a personal data breach. For this purpose, all METRO data protection officers are provided an organizational diagram that explains the steps required to involve the relevant operational departments.

39. Personal data breaches that could result in a risk to the rights and freedoms of data subjects are reported to the competent authorities within 72 hours pursuant to Article 33 GDPR. The data protection officer at the respective METRO Company is responsible for timely reporting. In order to ensure compliance with this deadline, data protection officers must be provided access to the official in-box, including on mobile devices, and a deputy must be designated in the case of absence who likewise must be provided access to the official in-box (at least during the period of absence).

40. Personal data breaches that could result in a high risk to the rights and freedoms of data subjects must be disclosed to the data subjects pursuant to Article 34 GDPR. The corporate communications department is required to be involved in cases where not all data subjects can be notified directly. This is also the case where publicity related to a personal data breach has or could result in reputational damage for METRO. The data protection officer may use forms and sample letters available to them in order to notify data subjects.

41. Every suspected personal data breach must be recorded and documented along with all communications with reporting parties, operational departments, supervisory authorities and data subjects. Similarly, all measures for containment, risk minimization and resolution of the personal data breach that have been planned or implemented must be documented by the data protection officer. Related documentation (see above) must be updated if such measures result in changes to technical and/or organizational measures. If such measures result in changes to the record of processing activities this must likewise be updated. Revisions are monitored by the relevant data protection officer.

42. All operational departments are obliged to report the number of personal data breaches occurring within their department to the data protection officer at the end of each fiscal year. A zero report must be provided in the event there are no data protection incidents. The relevant data protection officer is obliged to include all personal data breaches occurring during the fiscal year in their annual activity report.

Data Processors and Dealing with External Service Providers

43. METRO concludes appropriate agreements with all data processors. The DPD provides samples which are to be used by the operational departments in consultation with the relevant data protection officer. Departures from the minimum contents set out in Article 28 GDPR are prohibited. Additional requirements are set out in Annex 1 to the Data Protection Guideline. The relevant data protection officer is responsible for monitoring and concluding all required agreements for data processing with the relevant minimum contents.

44. Data processors with whom an agreement is to be concluded must, prior to conclusion of an agreement, provide a meaningful statement regarding appropriate technical and organizational measures they have taken in relation to the processing risk. The relevant data protection officer is responsible for reviewing the appropriateness of such measures. As part of this process, they may involve additional operational departments and utilize work instructions related to the review

of appropriateness of technical and organizational measures provided by the DPD. METRO will conclude data processing agreements upon approval of the to-be-agreed technical and organizational measures to be warranted by the data processor by the relevant data protection officer.

45. METRO Companies review and inspect data processors which process personal data on their behalf. Reviews and inspections are conducted on a risk-based approach and are initiated and supported by the data protection officer in relation to data protection issues.

46. All data processing agreements for METRO Companies must be retained so that they may be accessed at any time. The relevant METRO Company is responsible for ensuring compliant retention. The data protection officer for the respective METRO Company and the relevant data protection manager must be assured access to these agreements at any time.

Transfers to Third Countries

47. METRO is an internationally active Group with customers and partners around the world. METRO ensures that personal data is protected against external access, loss and modification when being transferred to other METRO Companies located abroad by means of technical and organizational measures. All METRO Companies must guarantee an adequate level of data protection and implement the requirements of the Data Protection Guideline.

48. When transferring personal data to third parties in third countries METRO ensures that there is an appropriate level of data protection in the destination country. The relevant data protection officer is responsible for conducting this review. If there is no adequate level of data protection pursuant to Article 45 GDPR, a review must be conducted to determine whether appropriate guarantees are in place or must be agreed with the recipient pursuant to Articles 40, 42, 46, 47 GDPR, or whether an exception pursuant to Article 49 GDPR may apply.

49. The transfer of personal data to third countries is reviewed together with the examination of the respective process and the record of processing activities as described above.

Communication

Communication Measures Related to Data Protection

1. METRO is making efforts to increase awareness of data protection among all employees. Secure and accessible communication channels are essential for these efforts.

2. METRO provides all employees information related to handling personal data on a regular basis via the Intranet, by e-mail, in teams and in printed form. This is intended to ensure that all employees have the ability to inform themselves about

the issue of data protection at any time. The Data Protection Guideline, including all Annexes, training materials, templates, fliers, updates and news that related to all METRO employees are communicated via the Intranet and are available there for all employees on a permanent basis. The data protection officers from all METRO Companies are advised to maintain their own pages on the Intranet on which they can communicate country-specific information related to data protection. Beyond this, data protection officers from METRO Companies are free to use other communications channels appropriate to their local conditions in order to raise awareness about the topic of data protection among company employees.

3. METRO supports communication between data protection officers and data protection coordinators within the Group and, in addition to information that is generally available on the Intranet, provides additional information in Microsoft Teams including a dedicated platform for purposes of communication.

4. METRO Companies set up official in-boxes in order to ensure availability of all data protection officers and provide access to data protection officers and their deputies. The address for these official in-boxes must be published in all privacy policies for the respective company and communicated to all employees.

5. Employees may contact the data protection officer at any time whether in person, by telephone or e-mail. Customers may make contact electronically using the official in-box, by telephone or via regular mail.

6. Rules concerning data protection are available on the Intranet and are distributed by e-mail. A wide variety of communications tools are available for communicating these rules. E-mail and document templates, sample contracts, check lists and brochures related to the most important data protection issues are made available. Additional information is available at training courses, from training materials and individual recommendations from managers.

Training Concept

7. All employees must receive training regarding the general handling of personal data. The data protection officer for the respective METRO Company is responsible for training employees, data protection coordinators and process owners. Participation in such general training courses is mandatory for all employees. The data protection officer is responsible for ensuring that employees who are obliged to participate do so. The data protection officer is required to offer sufficient training dates for employees so that they may all attend. The relevant superior is to be notified if employees fail to participate on multiple occasions. The continued refusal to participate may have employment-related consequences. General training courses must be repeated every two years.

8. METRO DPD provides both general and specialized training course content. The data protection officer for the respective METRO Company is responsible for disseminating this content.

Reporting

9. Data protection officers are obligated to report to their respective company and data protection manager annually following the close of the fiscal year about their work and the status of implementing data protection within their company.

10. The competent data protection manager is required to report to the METRO Board of Directors annually following the close of the fiscal year about their work and the status of implementing data protection at all companies for which they are responsible.

11. In addition, data protection officers must inform and consult with the boards of directors of the companies for which they have been named concerning risks and the status of implementation on a regular and ad hoc basis.

Monitoring and Improvement

Monitoring and Improvement Concept

1. The Group Board of Directors and the Board of Directors for each respective METRO Company are responsible for monitoring data protection. They may delegate this duty to data protection managers and data protection officers; however, they remain responsible for monitoring and controlling tasks they have delegated as described in Annex 2 to the Data Protection Guideline.

2. The competent data protection manager monitors the work of the data protection officer. For this purpose, the data protection manager may instruct the data protection officer to report on the status of implementing applicable data protection laws on a regular basis. In this context, the competent data protection manager is addressing the risks faced by the METRO Companies concerned of damage resulting from deficient implementation of applicable data protection laws and regulations.

3. The data protection officer monitors compliance with applicable data protection laws and regulations by the METRO Company that appointed them. To this end, the data protection officer conducts periodic efficiency testing as needed and/or random sampling controls of technical and organizational measures that have been implemented and the underlying concept, keeping the record of processing activities, and contracts with data processors and, if applicable, additional relevant documents. As needed, the data protection officer may involve the data protection manager in this review. The data protection officer reports on the results of this review as described in the section on reporting.

4. Independent audit conducted by Internal Audit, or auditing firms, ensure the independent review of work performed by the data protection officer and the data protection manager.

5. The data protection officer and the competent data protection manager are to be involved in the planning, preparation and performance of an audit if an audit conducted by Internal Audit is not intended to provide a review of the overall DMS but rather are focused on other tasks within the company and nonetheless relate to applicable data protection laws and regulations. Internal Audit is responsible selecting areas to be audited. The report is to be provided to the data protection officer and the competent data protection manager for information purposes following conclusion of the audit. The data protection officer is responsible for monitoring the implementation of recommended measures.

6. Information garnered from the audit and regular reviews by the data protection manager and the data protection officer are used by the DMS for purposes of updates and improvements.

Further Development of the DMS and Analysis of Potential for Improvement

7. Data protection related rules and policies are updated to reflect changes in the law or organizational and technical changes as part of the periodic-cyclical optimization process for data protection management (Plan-Do-Check-Act).

8. Knowledge included in the required documentation for a process, the associated risk assessment, personal data breaches, current training courses, publications and other sources are used in order to define follow-up measures. The intent of follow-up measures is to improve data protection and may include training, working documents, new technical and organizational measures to be implemented in order to protect personal data or changes to the data protection rules and policies. They are reported directly to the relevant person responsible by the data protection managers or data protection officers (see Structural and Process Organization) and monitored accordingly.

9. The respective boards of directors are involved in the monitoring and improvement process. Measures defined by the relevant managers may also be directed to the board of directors. The board of directors may accordingly also be the addressee of the measure concerned. In addition, deficiencies and any needed improvements are reported to the board of directors on, at least, an annual basis.

Düsseldorf, April 30, 2020

* *