欧盟数据保护准则
EU

Mercedes-Benz

目录

1 准则的目标 **4**

2 适用范围 **4**

3 梅赛德斯-奔驰集团内部的法律约束力 **5**

4 与法律要求的关系 **5**

5 处理个人数据的一般原则 **5**
- 5.1 合法性 5
- 5.2 有法律依据的客户和合作伙伴数据 5
  - 5.2.1 合同关系数据的处理 5
  - 5.2.2 出于广告宣传目的处理数据 6
  - 5.2.3 同意数据处理 6
  - 5.2.4 根据法定授权或义务的数据处理 6
  - 5.2.5 基于合法权益的数据处理 6
- 5.3 有法律依据的员工数据 6
  - 5.3.1 雇佣关系数据的处理 6
  - 5.3.2 根据法定授权或义务的数据处理 6
  - 5.3.3 有关数据处理的集体协议 6
  - 5.3.4 同意处理数据 7
  - 5.3.5 基于合法权益的数据处理 7
- 5.4 高度敏感数据的处理 7
- 5.5 自动化个人决策制定（可包括数据分析） 7
- 5.6 告知义务/透明度 7
- 5.7 目的限制 7
- 5.8 数据最小化 8
- 5.9 数据准确性 8
- 5.10 Privacy by Design 和 Privacy by Default 8
- 5.11 删除和匿名化 8
- 5.12 处理的安全性 8
- 5.13 梅赛德斯-奔驰集团外的（进一步）传输 9

6 数据保护影响评估 **9**

7 数据处理程序记录 **9**

8 委托处理 **10**
- 8.1 概述 10
- 8.2 对委托方的规定 10
- 8.3 关于集团内部受托方的规定 10

9 联合控制 **11**

10 数据主体可行使的权利 **11**
10.1 数据主体权利 11
10.2 投诉程序 11

11 责任和管辖地 **12**
11.1 责任规定 12
11.2 管辖地 12

12 数据保护事件报告 **12**

13 数据保护组织与惩罚措施 **12**
13.1 责任 12
13.2 意识提高和培训 13
13.3 组织 13
13.4 惩罚措施 13
13.5 审计和控制 13

14 对本准则的修订以及与政府机构的合作 **14**
14.1 修订时的责任 14
14.2 与政府机构的合作 14
14.3 第三国/地区法规的监测和报告 14

1 准则的目标

梅赛德斯-奔驰集团将数据保护视为其社会责任的一部分。

在一些国家和地区，如欧盟，立法机构规定了保护自然人数据（“个人数据”）的标准，包括要求只有在接收方目的地能提供适当的数据保护水平的情况下，才可将这些数据传输至该等国家/地区。

本欧盟数据保护准则就以下方面在集团内部建立了统一适用的数据保护标准：
- （a）在欧盟/欧洲经济区（EWR）（以下统称**“EU/EWR”**）等地区内处理个人数据以及
- （b）向 EU/EWR 以外的集团公司跨境传输个人数据（包括后续在目的地的数据处理）。

为此，本准则制定了梅赛德斯-奔驰集团内部处理来自 EU/EWR 的个人数据的约束性规则。该等规则称为梅赛德斯-奔驰集团的具有约束力的公司规则（“Binding Corporate Rules – BCR”），为保护 EU/EWR 以外的个人数据提供充分保障。

2 适用范围

本欧盟数据保护准则适用于梅赛德斯-奔驰集团股份公司、其受控集团公司（以下简称集团公司）及其员工和管理机构成员。在本欧盟数据保护准则中，“受控”是指梅赛德斯-奔驰集团股份公司可以直接或间接通过其多数投票、多数管理层代表或协议来要求采用本准则。

除非国家法律具有更广泛的规定，本准则适用于个人数据归档系统中的全部或部分自动化处理和手动处理。本准则也适用于德国境内所有硬拷贝格式的员工数据[1] 。
本准则适用于以下公司的个人数据的处理：
- （a）位于 EU/EWR 境内或本准则可以扩展到的其他国家/地区的集团公司及其分公司，（“位于 EU/EWR 境内的公司”），
- （b）位于 EU/EWR 境外的集团公司：为 EU/EWR 境内的自然人提供商品或服务的集团公司；和/或监控 EU/EWR 境内自然人行为的集团公司（“为 EU/EWR 提供产品的第三国/地区公司”）或者
- （c）位于 EU/EWR 境外的集团公司：直接或间接从 a）或 b）项下受本准则约束的公司接收个人数据的集团公司；或已向其披露该等数据的集团公司（“从 EU/EWR 获取数据的第三国/地区公司”）。

在本准则中，EU/EWR 境外的数据处理称为在第三国/地区处理。

参与或接受第三国/地区公司数据处理的集团公司列在其他适用的规定“受欧盟数据保护准则约束的集团公司名单”中。

本准则可扩展至 EU/EWR 境外的国家或地区。对于法律实体数据与个人数据受到同样保护的国家/地区，本准则同样适用于法律实体数据。

[1] 出于语言简化的原因，本准则中对自然人仅使用男性形式表示。在内容上是指所有性别身份的人。

3 梅赛德斯-奔驰集团内部的法律约束力

本准则的规则和规定对在其适用范围内运营的所有集团公司均具有约束力。因此，除适用的欧盟法规和国家数据保护法外，集团公司及其管理层和员工还应负责遵守本准则。

如果法律要求未作另行规定，集团公司无权采用与本准则相悖的规定。

4 与法律要求的关系

本准则不得取代欧盟法规和国家法律。其只作为国家数据保护法的补充。如果遵守本准则将导致违反国家法律，则应以国家法律法规为准。在国家法律未作规定的情况下，须遵守本准则的内容。

如果遵守本准则将导致违反国家法律，或者如果本准则与国家法律所要求的规则相悖，则必须向集团数据保护专员和总部合规组织报告，以便对数据保护法进行监测跟进。如果国家法律与本准则存在冲突，集团数据保护专员和总部合规组织应与负责的集团公司合作，寻找能够实现本准则目的的切实可行的解决方案。

5 处理个人数据的一般原则

5.1 合法性

必须以合法公正的方式收集和处理个人数据。只有在处理活动具有充分法律依据的情况下，才能进行数据处理。这也适用于集团公司之间的数据处理。单凭传输方公司和接收方公司均隶属于梅赛德斯-奔驰集团这一事实，并不足以证明数据处理的合理性。

有下列第 5.2 或 5.3 条项下的授权情形之一的，个人数据处理合法。如果个人数据处理目的脱离了最初目的，则在该等情形下也须获得许可。

5.2 有法律依据的客户和合作伙伴数据

5.2.1 合同关系数据的处理

相关潜在客户、客户或合作伙伴的个人数据处理允许用于订立、履行和终止某项合同。该等处理如果与合同目的有关，则还包括根据合同为客户或合作伙伴提供咨询服务。

在签订合同之前，可出于编制投标书或采购单，或满足潜在客户有关合同订立的其他要求，对个人数据进行处理。在合同启动过程中，可使用潜在客户提供的信息联系潜在客户。须遵守潜在客户要求的任何限制条件。

5.2.2 出于广告宣传目的处理数据

如果数据主体联系集团公司，向其提出信息相关要求（例如，要求提供有关要发送的产品的信息材料），则可对个人信息进行处理，以满足该等要求。客户忠诚或广告宣传措施须受进一步法律要求的约束。个人数据可出于广告宣传目的或市场和意见调查目的进行处理，但须与最初收集数据的目的一致。将数据主体的个人数据用于广告宣传的，则须事先告知数据主体。如果仅出于广告宣传目的收集数据，则数据主体可选择是否提供该等数据。应告知数据主体，其可自愿出于该等目的提供数据。数据主体同意是数据传输过程的构成部分，应事先获取数据主体同意。在获得同意后，应向数据主体提供可用的联系方式，如电子邮件和电话（有关同意，请参见 5.2.3 条），供其选择。如果数据主体不同意将其数据用于广告宣传目的，则应不再出于该等目的使用该等数据，且须限制或禁止数据的任何该等使用。关于数据用于广告宣传目的，须遵守特定国家/地区的任何其他相关限制。

5.2.3 同意数据处理

数据处理可在获得数据主体同意后进行。在同意作出前，须根据本欧盟数据保护准则通知数据主体。同意声明须以书面或电子方式获得，以作归档。在某些情况下，也可通过口头表示，如电话交谈获得同意。同意意见须记录在案。

5.2.4 根据法定授权或义务的数据处理

如果国家立法要求、需要或准许，则也允许进行个人数据处理。数据处理的类型和范围须符合法律允许的数据处理要求并符合相关的法律规定。

5.2.5 基于合法权益的数据处理

如果合法权益需要，则也可对个人数据进行处理。合法权益通常是合法的（如未清应收款的收取）或商业性的（如避免违约）。如果在特定情况下，数据主体在保护其数据方面的权益超过了数据处理过程中的合法权益，则不得依据该等合法权益进行数据处理。在数据处理之前，有必要确定是否存在值得保护的数据主体权益。

5.3 有法律依据的员工数据

5.3.1 雇佣关系数据的处理

对于雇佣关系，如果需要建立、履行和终止雇佣关系，则可对个人数据进行处理。对求职者个人数据进行处理有助于决定是否建立雇佣关系。如果求职者未被录用，除非该求职者同意为以后的候选程序继续保存其数据，否则须在证据法规定的期限内删除该等数据。将数据用于其他求职流程或将求职材料转发给集团其他下属公司前，也需要征得求职者同意。在现有的雇佣关系中，如果数据的授权处理不符合以下任一情形的，须始终与雇佣关系的目的相关联。

如果在雇佣关系建立阶段或在现有雇佣关系中需要由第三方收集求职者的其他信息，则须遵守相应国家的法律要求。如有疑问，在允许的情况下，应征得数据主体的同意。

对最初并非出于建立或终止雇佣关系而收集的、但又与雇佣关系有关的个人数据（员工数据）进行处理时，须具有以下所列的法律依据。

5.3.2 根据法定授权或义务的数据处理

如果国家立法要求、需要或准许，则也允许进行员工数据处理。数据处理的类型和范围须符合法律允许的数据处理要求并符合相关的法律规定。如果法律存在一定的灵活性，则须考虑员工的受保护权益。

5.3.3 有关数据处理的集体协议

如果数据处理活动超出合同的履行目的范围，但经集体协议授权，则该等活动仍被允许。相关授权规定须涵盖所需进行的数据处理的具体用途并在欧盟法规和国家法律要求的范围内进行制定。

5.3.4 同意处理数据

员工数据可在获得数据主体同意后进行处理。同意声明书须自愿提交。拒绝提交同意声明的，不得受到任何处罚。非自愿的同意为无效同意。同意声明须以书面或电子方式获得，以作归档。在特殊情况下，如果条件不允许以上述方式作出同意，可以口头作出同意。同意的授予在任何情况下均须记录在案。在同意作出前，须根据本欧盟数据保护准则通知数据主体。

5.3.5 基于合法权益的数据处理

如果集团公司合法权益需要，则也可对员工数据进行处理。合法权益通常是合法的（例如主张、行使或捍卫法律索赔要求）或商业性的（例如加快业务流程、对公司进行评估）。在数据处理之前，有必要确定是否存在值得保护的数据主体权益。如果值得保护的员工权益小于数据处理的合法权益，则可基于合法权益进行个人数据处理。

除非有法律义务或正当理由，否则不得就除履行雇佣关系（如绩效检查）以外的员工数据处理要求采取控制措施。即使有正当理由，也须对控制措施的相称性进行审查。为此，须权衡集团公司在执行控制措施时的合法权益（如遵守法律规定和公司内部规则）与受该措施影响的员工在不执行该等措施的情况下可能拥有的任何受保护权益。该等措施只有在具体情况下且适当时才可采取。采取任何措施之前，须确定是否存在集团公司的合法权益以及任何值得保护的员工利益，并进行存档。此外，须考虑是否存在适用法律下的任何附加要求（例如，员工代表的共同决定权和数据主体获取信息的权利）。

5.4 高度敏感数据的处理

高度敏感数据的处理须经国家法律明确许可，或按照国家法律的明确规定进行。在以下特殊情况下，可允许集团公司对高度敏感数据进行处理：已获得数据主体的明确同意；数据处理对主张、行使或为与数据主体有关的法律索赔进行抗辩是必要的；或者数据处理对管理者履行其在劳动就业法方面的权利和职责是必要的。

如果有计划要对高度敏感个人数据进行处理，则须事先通知集团数据保护专员。

5.5 自动化个人决策制定（可包括数据分析）

只有在订立或履行合同有需要，或数据主体已同意时，才可对数据主体进行可能对其产生法律或类似负面影响的完全自动化决策。在某些情况下，该等自动化决策可包括数据分析，即评估个人人格特征（如信誉）的个人数据处理。在这种情况下，须通知数据主体自动化个人决策的生成和结果，并向数据主体提供机会，由管理者对其进行个人审查。

5.6 告知义务/透明度

负责的专业部门须根据通用数据保护条例（GDPR）第 13 条和第 14 条的规定，将处理个人数据的目的和情况告知数据主体。如果该等数据不在通用数据保护条例（GDPR）的适用范围内，则须根据适用的国家法律规定进行告知。须以准确、简洁、易懂、易于获取的形式和清晰、通俗的语言进行告知。须遵守集团数据保护专员和数据合规部门的规定。首次收集个人数据时，须向数据主体提供该等信息。如果集团公司从第三方接收个人数据，除非出现以下情况，否则须在获得数据后的合理期限内向数据主体提供该等信息：

- 数据主体已经拥有该等信息；或者
- 无法向数据主体提供该等信息；或者
- 提供该等信息极其困难。

5.7 目的限制

仅能出于资料收集前所确定的合法目的，对个人数据进行处理。只有在个人数据的处理与其最初的收集目的相符的情况下，才允许对处理目的进行后续更改。

5.8 数据最小化

对个人数据的任何处理，不论是在数量上，还是在质量上，均须限制在为达到合法处理该等数据的目的所需的范围内。这一点须在最初的数据收集过程中予以考虑。如果处理是在目的所需范围内，且所付出的努力与所追求的目的相称，则须使用匿名或统计数据。

5.9 数据准确性

储存的个人数据须客观正确，如有必要，还须是最新数据。须采取适当措施，确保对不正确或不完整的数据进行删除、更正、补充或更新。

5.10 Privacy by Design 和 Privacy by Default

“Privacy by Design”原则旨在确保各专业部门在概念化和技术设计阶段的一开始，就制定最先进的内部策略，并采取措施将数据保护原则整合到业务模型/流程和 IT 系统的规范和架构中，以便进行数据处理。按照“Privacy by Design”的原则，个人数据处理程序和系统的默认设置须设计成仅限于实现数据处理目的所需的数据处理（“Privacy by Default”原则）。这包括处理范围、存储周期和可访问性。进一步措施可包括：

- 尽快将个人数据假名化
- 将个人数据的功用和处理透明化
- 允许数据主体决定其个人数据的处理
- 使程序或系统的操作人员能够设计和增强安全功能。

各集团公司应在数据处理活动的整个周期内实施并保持适当的技术和组织措施，以确保始终遵守上述原则。

5.11 删除和匿名化

个人数据只可在实现数据处理目的所需的期间内储存。这意味着，除非文件存档或保存义务继续适用，否则个人数据须在处理目的实现或失效后立即删除或匿名化。负责各个程序的人员必须确保对其程序执行常规删除和匿名化处理。每个系统必须有一个手动或自动删除例程。数据主体通过删除或移除个人标识符而提出的删除要求必须在系统内技术上可行。必须遵守梅赛德斯-奔驰集团股份公司对执行删除例程（例如软件工具、概念删除执行小册、归档要求）的要求。

5.12 处理的安全性

必须保护个人数据，以防止未经授权查阅、非法处理或转移，以及意外遗失、更改或销毁。在引入新的数据处理方法（尤其是新的 IT 系统）之前，必须确定并实施保护个人数据的技术和组织措施。这些措施必须以技术水平、处理风险和保护数据的需要为基础。

与数据保护有关的技术和组织措施必须由管理者在数据保护影响评估和程序概要的范围内予以记录。

特别是，负责的专业部门必须咨询其业务信息安全官（BISO）、信息安全官（ISO）及其数据保护网络。保护个人数据的技术和组织措施要求是公司信息安全管理的一部分，并且必须根据技术发展和组织变化不断进行调整。

5.13 梅赛德斯-奔驰集团外的（进一步）传输

向集团公司外或集团公司内的接收方传输个人数据，须遵守第 5 条处理个人数据的授权规定。必须要求数据接收方仅将数据用于指定的用途。

如果要跨境传输个人数据（包括允许从另一个国家/地区进行访问），则必须满足有关个人数据境外传输的相关国家要求。特别是，EU/EWR 的个人数据只有在接收方能够证明其具有与该准则等效的数据保护级别时，才能在集团公司以外的第三国/地区进行处理。适用的证明可以是：

- 欧盟标准合同协议条款，
- 接收方参与欧盟认可的认证体系，确保能充分保护数据，或
- 确认接收方具有约束力的公司规则，以由负责的监督机构提供适当水平的数据保护。

不得大规模、不成比例和不加选择地，在民主社会所必需的数据披露范围外，向任何政府机构传输个人数据。一旦这些要求与政府机构要求发生冲突，梅赛德斯-奔驰集团股份公司将与相关集团公司合作，找到一个切实可行的解决方案，以实现本准则的目的（第 14.3 条）。

第 5 条所列的所有责任均为数据主体的第三方受益人权利。

6 数据保护影响评估

集团公司在采用新处理方法、或在对现有处理方法进行重大更改（尤其是通过使用新技术）时，应评估该处理方法是否会对数据主体的隐私造成高风险。此时必须考虑数据处理的性质、范围、背景和目的。作为风险分析的一部分，负责的专业部门应对计划的处理方法对个人数据保护的影响进行评估（数据保护影响评估）。如果在进行数据保护影响评估并采取适当的降低风险措施后，数据主体的权利和自由仍存在高风险，则须告知集团数据保护专员，以便其可以咨询主管的数据保护监督机关。必须遵守梅赛德斯-奔驰集团股份公司为执行此评估（如软件工具、评估执行说明等）制定的规定。

7 数据处理程序记录

每个集团公司必须将处理个人数据的程序记录在程序概要中。程序概要须以书面形式保存，可采用电子格式，并根据要求提供给数据保护监督机关。必须遵守梅赛德斯-奔驰集团股份公司制定的文件记录规定（如软件工具和文档说明）。

8 委托处理

8.1 概述

委托处理是指当受托方以服务供应商的身份，代表和根据委托方的指示处理个人数据。在这些情况下，必须根据相关的法律要求与外部受托方以及梅赛德斯-奔驰集团内的集团公司签订委托处理协议（例如“委托处理协议”模板）。委托方全权负责数据处理的正确执行。

第 8.3 条的规定也适用于非集团公司的外部委托方。

8.2 对委托方的规定

进行委托时，必须遵守下列规定，即发出委托的专业部门必须确保符合下列规定：

- 必须根据其是否适合确保必要的技术和组织保护措施来选择受托方。
- 必须遵守集团数据保护专员提供的数据保护合同标准。
- 委托必须以书面或电子形式发出。应以文件形式记录数据处理指示、委托方与受托方的责任。

在数据处理开始之前，委托方必须通过适当的评估确认受托方可履行上述义务。必须遵守梅赛德斯-奔驰集团股份公司为执行此评估（如软件工具、评估执行说明、合同范本等）制定的规定。受托方可以记录其对数据保护要求的遵守情况，特别是通过提供适当的证明。根据数据处理的风险，必须在合同期内定期重复进行检查。

8.3 关于集团内部受托方的规定

受托方仅允许在委托方的指示下处理个人数据。

只有在获得委托方事先同意的情况下，受托方才可以委托其他集团公司或第三方（“分包商”）根据其自己的（分包）合同处理个人数据。受托方只有在根据本准则，针对集团公司和数据主体要求分包商以合同或其他类似的法律约束手段承担相同的数据保护义务并采取适当的技术和组织保护措施的情况下，才能获得同意。如果分包关系发生变化，必须在服务合同中规定同意形式和告知义务。

受托方有义务为委托方提供适当的支持，以遵守适用于委托方的数据保护规定，特别是通过提供所有必要的信息。这特别关系到保障以下事项：

- 第 5 条项下的一般处理原则
- 第 10 条项下的数据主体权利
- 第 12 条项下的委托方告知义务
- 第 8 条项下对委托方和受托方的规定
- 以及监督机构对征询和调查的处理。

如果适用的标准或法律规定要求受托方违反委托方的指示进行处理，或者，如果这些条款妨碍受托方履行其在本准则或委托处理协议项下的义务，受托方应立即通知其委托方，除非相关法律规定禁止发出通知。如果受托方由于其他原因不能遵守委托方的指示，则适用此规则。在这种情况下，委托方有权暂停数据传输和/或终止委托处理协议。

受托方有义务将政府机构提出的有关披露个人数据的任何具有法律约束力的要求告知委托方，除非因其他原因禁止告知。

根据委托方的选择，受托方必须在服务履约终止时删除或归还委托方提供的所有个人数据。

受托方有义务将数据主体提出的任何索赔、要求或投诉立即通知委托方及其客户（如适用）。

集团内部委托方还必须强制外部受托方遵守上述规定。

受托方对委托方的具体职责是数据主体的第三方受益人权利。

9 联合控制

如果多个集团公司（如适用，与一个或多个第三方）（联合控制者/Joint Controller）共同确定个人数据的处理方法和目的，则这些公司必须订立协议，规定其对处理数据主体数据的职责。必须遵守集团数据保护专员提供的合同范本。

10 数据主体可行使的权利

第 10 条所列数据主体的所有权利及集团公司的义务，均为该数据主体的第三方受益人权利。

根据第 10 条提交的请求和投诉，须在一个月内予以答复。考虑到请求的复杂性和数量，可以在一个月的基础上再延长最多两个月，同时必须相应通知数据主体。

10.1 数据主体权利

EU/EWR 境内的数据主体对各个负责的集团公司，或（如果是受托方）对委托方享有以下权利（具体请参见欧盟法律的详细规定）：

- 有权获知其个人数据处理情况。必须遵守集团数据保护专员对该等告知的要求。
- 获取有关其数据处理方式信息的权利，以及其在这方面有权享有的权利。如果雇主有根据相关雇佣法查阅有关雇佣关系的文件（例如人事档案）的权利，则这些权利不会受影响。根据要求，数据主体可获得其个人数据的复本（可能须支付合理的费用），除非值得保护的第三方利益禁止这种行为。
- 如果个人数据不正确或不完整，有更正或补充的权利。
- 如果其撤回自己的同意或法律依据已不再适用，则有删除个人数据的权利。如果数据处理背后的目的由于其他原因已经失效或不再适用，也同样适用。必须遵守禁止删除的现有保留期限和值得保护的利益。
- 如果数据主体对其数据的准确性有异议，或者如果集团公司不再需要该数据，但数据主体需要该数据以满足其法律诉求，则其有限制处理其数据的权利。如果必须删除该数据，或正在复核数据主体的反对意见，数据主体也可以要求集团公司限制其数据的处理。
- 获取与其有关的个人数据的权利，这些数据是在获得其同意的基础上，或在与其签订或发起的协议之情形下，以常用的数字格式提供的；如果数据是通过自动化方式处理的，而且技术上是可行的，则其也有将这些数据传送给第三方的权利。
- 随时反对直接营销的权利。必须确保具有适当的同意和反对管理。
- 因其特殊的个人情况，反对在集团公司或第三方压倒一切利益的法律基础上处理个人数据的权利。但是，如果集团公司有令人信服的理由进行处理，或该数据正被处理以确立、行使或抗辩法律申索，则这项反对权不适用。如果有合理的反对意见，则必须删除数据。

此外，数据主体也有权向在第三国/地区导入数据的集团公司主张其权利。

10.2 投诉程序

如果数据主体认为本准则已被违反，其有权向集团数据保护专员投诉。此类投诉可以通过电子邮件提交。

位于 EU/EWR 境内作为数据导出方的集团公司将依据本准则协助其个人数据在 EU/EWR 境内被收集的数据主体确定事实，并向导入数据的集团公司主张权利。

如果数据主体不同意集团公司关于是否符合要求的决定（或因其他原因对处理不满意），其可以通过行使权利质疑该决定或行为。为此，其可向其经常居住地、工作地或涉嫌违规的行为发生地的主管监督机构提出申请，或向法院提起诉讼（第 11.2 条）。其他法定权利和责任不受影响。

11 责任和管辖地

11.1 责任规定

如果位于 EU/EWR 境内的集团公司（“数据导出者”）首先将个人数据传输至位于第三国/地区的集团公司，则其对从 EU/EWR 接收数据以供第三国/地区处理的第三国/地区公司的任何违反本准则的行为承担责任。该责任包括补救非法情况的义务，以及赔偿因第三国/地区集团公司违反本准则而造成的物质和非物质损害的义务。

只有在能够证明接收来自 EU/EWR 的数据的第三国/地区集团公司对造成损害的行为不承担责任的情况下，数据导出者才能免于承担部分或全部责任。

11.2 管辖地

数据主体可以向控制者或受托方所在地或常住地的法院提起诉讼。

在第三国/地区处理的情况下，声称违反本准则的数据主体可以对 EU/EWR 境内的数据导入和数据导出公司主张其法律诉求。数据主体可以将被指控的侵权行为和由此产生的法律索赔提交控制者所在地或控制者常住地的主管法院和监管机构。

本条关于责任和管辖地的规定是数据主体的第三方受益人权利。

12 数据保护事件报告

如果发生可能违反数据安全要求的事件（“数据保护事件”），则涉事集团公司有调查、通知和减轻损害的义务。数据保护事件是指数据泄露，即存在违反安全规定导致个人数据被非法销毁、更改、未经授权披露或使用的事件。如果个人数据泄露很可能导致自然人的权利和自由受到威胁，则通常必须在初次发现后的 72 小时内将相应的违规行为告知主管监督机构。此外，必须告知数据主体任何可能对其权利和自由构成高风险的数据泄露情况。第 8.2 条中所指的受托方有义务立即向其委托方报告数据保护事件。

如果在集团公司的责任范围内发现或怀疑发生了数据保护事件，每位员工均有义务按照信息安全事件管理流程立即报告。必须遵守梅赛德斯-奔驰集团股份公司在这方面规定的要求（例如软件工具、报告说明）。

任何数据泄露都必须记录下来，并且必须根据要求将记录提供给监督机构。

13 数据保护组织与惩罚措施

13.1 责任

集团公司管理机构的成员负责其职责范围内的数据处理。因此，他们需要确保满足数据保护方面的法律要求以及欧盟数据保护准则中包含的要求（例如，国家报告职责）。在他们的职责范围内，管理人员负责确保组织、人力资源和技术措施到位，以便根据数据保护要求进行任何数据处理。主管员工负责落实这些规定。如果政府机构进行数据保护检查，必须立即通知集团数据保护专员。

13.2 意识提高和培训

如果员工经常或定期访问个人数据、参与收集数据或参与开发处理个人数据的工具，则管理人员必须确保其员工接受及参加所需的数据保护培训，包括本准则的内容及处理方法。须遵守集团数据保护专员和数据合规部门的规定。

13.3 组织

集团数据保护专员在内部独立于有关其任务执行的指示。他必须确保遵守国家及国际数据保护法。他负责本准则并监督其遵守情况。如果集团公司希望参加某个国际认证体系以制定具有约束力的公司数据保护规则，则必须与集团数据保护专员就该参与行为协商一致。

集团数据保护专员由梅赛德斯-奔驰集团股份公司董事会任命，并在履行其职责时受董事会支持。一般来说，在法律上有义务任命数据保护专员的集团公司将任命集团数据保护专员。集团数据保护专员直接向梅赛德斯-奔驰集团股份公司董事会以及已任命集团数据保护专员的所有集团公司的相应管理层报告。特殊例外情况必须与集团数据保护专员达成一致。

应在现有报告义务范围内向梅赛德斯-奔驰集团股份公司监事会提交集团数据保护专员的年度报告。

所有数据主体可随时联系公司集团数据保护专员，就数据保护或数据安全问题表达他们的担忧，提出疑问，索取信息或提出投诉。如有要求，有关问题和投诉应进行保密处理。

集团数据保护专员的联系方式：

梅赛德斯-奔驰集团股份公司，集团数据保护专员，HPC E600，
70546 斯图加特，德国
电子邮箱：data.protection@mercedes-benz.com
内网：https://social.intra.corpintra.net/docs/DOC-71499

梅赛德斯-奔驰集团还建立了一个合规组织，在专门的内部规定中对其进行了更为详尽的描述。合规组织支持、监督集团公司对数据保护法的遵守情况，确定数据保护培训内容，并规定参与者群体的标准。

13.4 惩罚措施

根据许多国家/地区的监管法律和刑法规定，非法处理个人数据或违反数据保护法的其他行为可能会受到起诉，也可能引起索赔。根据雇佣法的规定，员工个人造成的违规行为可能会受到纪律处分。违反本准则的行为将根据内部规定予以惩罚。

13.5 审计和控制

应在集团级别对本准则和其他适用数据保护法的遵守情况进行定期、基于风险的审查，至少每年一次。通过内部合规风险评估、包括特定数据保护主题的审计和其他审查来实现这一点。集团数据保护专员有权要求进行进一步检查。审查结果须报于集团数据保护专员、相关集团公司及其数据保护专员（如有任命）。

作为现有报告职责的一部分，须向梅赛德斯-奔驰集团股份公司董事会报告重大审查结果。经要求，应向数据保护监督机构提交审查结果。数据保护主管监督机构可在国家法律规定的权力范围内，对各集团公司进行数据保护审计，以检查其对本准则规定的遵守情况。

14 对本准则的修订以及与政府机构的合作

14.1 修　订时的责任

本准则仅可在与集团数据保护专员协商一致后，通过规定的准则修订程序（用于准则管理的准则，A 1）予以变更。变更对本欧盟数据保护准则，A 17 造成重大影响或可能削弱本准则提供的保护水平的（即对约束力的变更），须立即报告给批准本准则作为具有约束力的公司规则的数据保护主管机构。

集团数据保护专员负责维护受本准则约束的所有集团公司的最新列表（其他适用的规定“受欧盟数据保护准则约束的集团公司名单”）。根据本准则，在新集团公司受到本准则的有效约束并考虑到遵守本准则的相关合规措施之前，不得向新集团公司传输个人数据。

数据主体有权随时访问本准则。本准则的最新版内容发布在 https://www.group.mercedes-benz.com 的数据保护项下。 此要求是数据主体的第三方受益人权利。

如果对本准则或受约束集团公司列表进行了修订，则集团数据保护专员应每年向梅赛德斯-奔驰集团股份公司总部监督机构发出一次修订通知，并简要说明修订原因。

14.2 与政府机构的合作

在第三国/地区或参与第三国/地区数据处理的集团公司有义务就上述情形下与个人数据处理有关的问题、问询或其他程序的相关事项，与主管监督机构进行合作。这包括有义务接受监督机构的合法审计。此外，基于第三国/地区的数据处理程序或本准则的规定，还应遵守主管监督机构的所有合法指示。

第 14.2 条关于与政府机构合作的规定是数据主体的第三方受益人权利。

14.3 第三国/地区法规的监测和报告

如果位于第三国/地区的公司合理预期存在欧盟及其成员国以外的国家或机构通过的、会造成以下风险的法律或其他法规，则该公司负责人须立即告知集团数据保护专员：

- 该等法律或法规将使相关第三国/地区公司或其他集团公司无法履行其在第三国/地区处理数据时本准则项下的义务；或者
- 该等法律或法规可能对本准则赋予数据主体在第三国/地区处理数据时的权利产生重大不利影响。尤其是在当地政府机构要求以超出民主社会所需范围的方式进行大规模、不成比例、不加区别的个人数据传输的情况下，应立即告知集团数据保护专员。

如果预计相关法律要求会在很大程度上对本准则提供的保护造成影响，集团数据保护专员应对该等影响进行评估，并通知数据保护监管机构（如适用）。本规定是数据主体的第三方受益人权利。

如果政府机构要求第三国/地区公司不得就个人数据披露告知数据保护监督机构，第三国/地区公司应采取一切适当措施，尽可能缓和或废除该等禁令，并向数据保护监督机构提供每年收到的该等披露要求的基本信息［例如，申请披露数量、申请披露的数据类型、申请者（如可能）］。

Mercedes-Benz Group AG, Mercedesstraße 120, 70327 Stuttgart, Germany, www.group.mercedes-benz.com