グローバルデータおよび情報規程 A 22.0

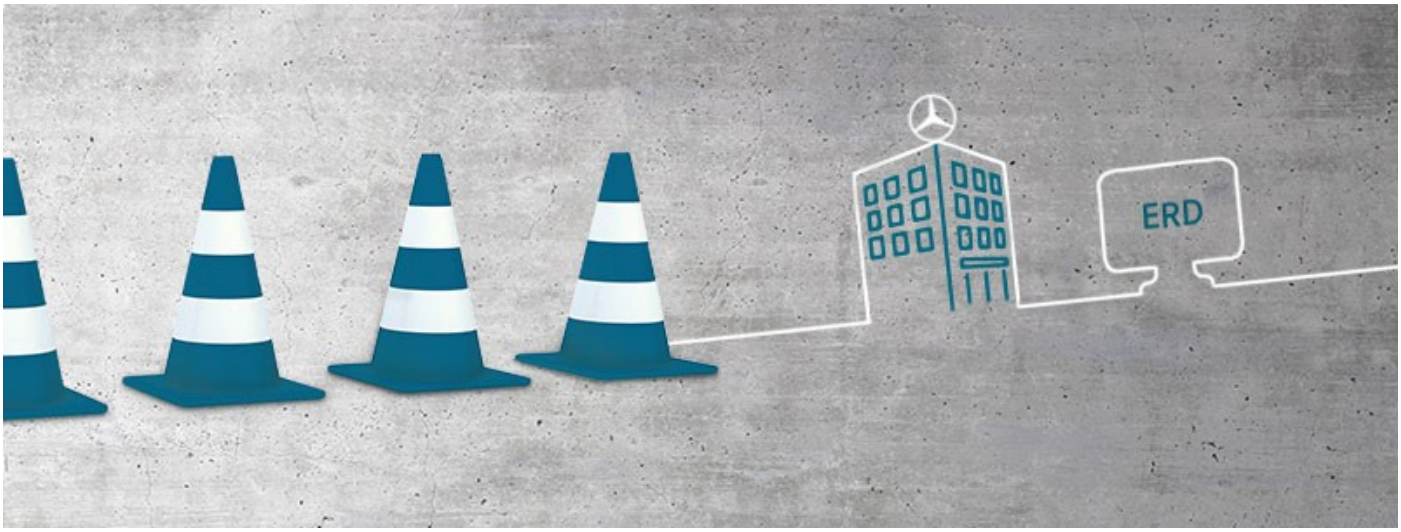
担当者

Sebastian Gress - IL/CD - Mercedes-Benz Group AG (0400)

規定責任者

Sebastian Gress - IL/CD - Mercedes-Benz Group AG (0400)

情報セキュリティ：Markus Schaub - HR/PSG - Mercedes-Benz Group AG



規定の目的/概要

本規程は、Mercedes-Benz Group内のデータおよび情報を、法令に遵守した上で、倫理的に正しく責任を持って取り扱うための基本となるものである。本規程では、データ化・情報化された環境下の責任と役割を明確化する。さらに、そのために必要なプロセスを確立すべく、必須となる目的、原則、組織構造および対策を定める。

上記についてデータマネージメント、データコンプライアンス、情報セキュリティの3種類のテーマ領域で説明する：

- データマネージメントは透明性を与え、データの利用を可能にする。
- データコンプライアンスは、法律に準拠した責任あるデータの取扱いを保証する。
- 情報セキュリティは、情報の安全性を確保する。

前回バージョンの変更

2022/06/01 – 改定：
リブランディング プロジェクトの一環としての適合

行動要件

グループ会社の経営組織メンバー対象

本規程をただちに公布・適用し、対象の従業員に通知してください。

Mercedes-Benz Group AGの管理職が対象

グローバルデータおよび情報規程 A 22.0

本規程の内容をよく理解し、これを遵守してください。

Mercedes-Benz Group AGの従業員が対象

本規程の内容をよく理解し、これを遵守してください。

Framework Light社の経営組織メンバー対象

これは必須方針です。貴社は、この規定の適用範囲に該当しています。この規定をすぐに発効していただくようお願い申し上げます。

規定を発効しない場合のリスク

Inadequate transparency, insufficient availability, unlawful, negligent or unsafe handling of information and data may lead to damages (including loss of trust and reputation) for the Mercedes-Benz Group.

適用範囲

本規程は、Mercedes-Benz Group AGおよび本社直轄のグループ会社全社の全従業員と経営陣メンバーに適用されます。

適用範囲の説明

データマネジメントの章に関して、データガバナンス委員会の決定に基づき各範囲ごとに定められた遅くとも 2022年12月31日までの移行期間があります。
詳細はこちらをご覧ください： グローバルなデータと情報規程 A 22 に同時に適用される規則と連絡先

有効期間

2020/01/22 - 2025/01/21

最終変更

2022/06/01

テーマ

企業統制 (データおよび情報)

承認

Renata Jungo Brüngger IL, Wilfried Porth HR
2020/01/15

文書

メルセデス・ベンツのソーシャル・イントラネットの企業方針データベース (ERD) で 2022/06/01 に公開。

必須文書

規定文書

グローバルデータおよび情報規程: 27 ページ数
付録1：用語集: 4 ページ数
付録2：Management Summary: 14 ページ数

グローバルデータおよび情報規程 A 22.0

同時に適用される規定

- IC 0.2 私たちのインテグリティ規程
- A 7.3 法人方針資料保管方針
- A 17.3 EUデータ保護規則
- A 32.1 IT端末およびカメラに関する規程
- グローバルデータおよび情報規程に関するロールハンドブック (English)
- データマネージメントガイドライン (English)
- マネージメントに対するデータCMS要件 (English)
- データ分析のためのコンプライアンスフレームワーク (English)
- データコンプライアンス対策 (English)
- 情報セキュリティ規則 (RISE) (German)
- グローバルなデータと情報規程 A 22 に同時に適用される規則と連絡先

目次

1 基本

1.1 序章

データおよび情報は、**Mercedes-Benz Group**[1]の戦略と運営において重要な役割を果たす。例えばバリューチェーン全体で発生する日常業務や当社の製品によって、さまざまな場所、多様な方法、異なる時点でデータや情報が発生する。

データおよび情報は、当社の既存プロセスの確立と改善の基礎となる一方で、新たな事業部門やモビリティコンセプトを立ち上げるためにも不可欠である。そうして、顧客に付加価値を提供する革新的なサービスと製品を実現できる。データと情報の正しい取扱いとそれらへの適切なアクセスが、重要な前提となる。当社の顧客と従業員[2]もまた、Mercedes-Benz Group で個人情報が安全に取り扱われることを望んでいる。

顧客と従業員は、Mercedes-Benz Group で個人情報が安全に取り扱われることを望んでいる。

例えば個人情報の不正な取扱いが、法律違反や Mercedes-Benz Group の信用を失うことにつながる場合がある。情報漏洩により、情報や知識が失われてしまうおそれがある。生産段階でデータが利用できなければ、製造ロスなどの原因となる場合がある。

1.2 目的

Mercedes-Benz Group は、法律を遵守し、倫理的に正しく責任を持ってデータと情報を取り扱う義務があり、データに対する責任を負う（*インテグリティ規程 (IC)* 参照）。本**グローバルデータおよび情報規程、A 22** には、以下の内容が含まれる：

- Mercedes-Benz Group の戦略的かつ有益な資源であるデータおよび情報の提供と処理に関する規則
- データ（個人情報またはその他のデータ）を法律に準拠し責任を持って取り扱うことを目的とする、データコンプライアンス（情報保護を含む）の国際基準
- 情報の適切な安全性を確保するための要件

本規程には、以下の関連規則が含まれる：

- データマネージメント
- データコンプライアンス
- 情報セキュリティ

さらに *EU データ保護規則、A 17* では、**特に EU 加盟国を中心に**、個人情報の取扱いに関する指針を定めている。

Mercedes-Benz Group の**すべての従業員**は、データおよび情報を規則に従って倫理的に正しく取扱い、保護する**責任を負う**。従業員には、本規程の要件を実践し、さらに担当部門の取り組みを支援することが義務付けられる。

Mercedes-Benz Group の**すべての管理職**は、各自の責任範囲において本要件を**実践し遵守する責任を負う**。

---

1 Mercedes-Benz Group：Mercedes-Benz Group AG 及び本社直轄のグループ会社

2 本規程では文章を分かりやすくするため、男女を区別した記載はしない。内容はどれもあらゆる性別を対象としている。「従業員」という用語には、全レベルの管理職と経営陣メンバーも含まれる。

1.3 データ取扱いに関するビジョン

「Mercedes-Benz Data Vision」と名付けられたデータ取扱いに関するビジョンでは、Mercedes-Benz Group がどのようにデータおよび情報を将来の機会のために利用するか、また顧客利益を保護するかについて説明する。当社の目標は、持続可能なデータベース型ビジネスモデルを実践することである。ここでの「持続可能」とは、法的要件を単に遵守するだけではなく、それ以上の責任を持ってデータを扱うことを意味している。同時に、ステークホルダーや利害関係者、そして何よりも顧客の要望を重視する。データ関連業務の基本となるのが、7 つの基本原則である（*インテグリティ規程 (IC)* および *データに関する責任*も参照）。

Mercedes-Benz のデータ取扱いに関するビジョンの焦点となるのは、責任あるデータの取扱いと顧客利益の保護である。

図 1 : データ取扱いに関するビジョンおよび 7 つの原則

これらの基本原則は、法律に準拠した、倫理的に正しいデータの責任ある取扱いについて説明している。

Mercedes-Benz のデータ取扱いに関するビジョンに基づく 7 つの基本原則。

- 当社がデータを利用する意図は、企業として**事業機会**を開拓するためである。これは当社が株主から期待されていることであり、同時に企業としての成長のために重要な要素でもある。
- 当社はデータによって利益または**顧客にとっての付加価値**を生み出そうとしている。つまり、さらなる快適性、新しい機能や体験を顧客が享受できるようにする。
- **質**の高い収集データのみが、顧客および事業に利益をもたらす。
- **透明性**は信頼を生む。そのため当社の顧客は、個人情報が収集される理由を知らされるべきである。また、社内においても透明性の確保が望まれる。どのようなデータが存在するのか理解していれば、目的に応じてデータを利用できるからである。
- 顧客が当社と個人情報の共有を望もうと望まざるとに関わらず、**選択の可能性**を常に用意しておく必要がある。選択は明確にし、できる限り容易に行えるようにする。
- **保護されたデータ**は、顧客の信頼の基本である。

- **データ倫理**：当社は、企業バリュー（*インテグリティ規程 (IC)* に定義されている）、企業方針および企業規則に一致した、責任ある行動を取る。

各原則の詳細は*第 3.1.1 章*で説明されている。

1.4 データおよび情報

Mercedes-Benz Group では、データおよび情報を以下のように理解する。

情報は企業資産である。

- **情報**とは主にデータに代表されるものであり、例えば知識、連絡、事実、意見、管理プロセスを伝えることができる。情報はさまざまな理由によって保護される。例えば戦略的に重要な情報（企業資産、業務上の機密事項を含む）、または個人情報 に該当する場合や、法律で保護された特許などがこれにあたる。情報には、デジタル形式、物理的形式、従業員の知識など、さまざまな形式のものが存在する[3]。

データとはデジタル形式の情報である。

- **データ**とは、主に増加傾向にあるデジタル形式の情報を指す。本規程に記載されている対策は、特に他のデータ形式を明記しない限り、デジタルデータの取扱いについて説明している。個人情報という用語は、媒体に依存しない自然人に関わるデータおよび情報全体を含んでいる。

データおよび情報はさまざまな形を取りながら、企業資産の部分集合を構成している。これらの関係性を図 2 に示す。

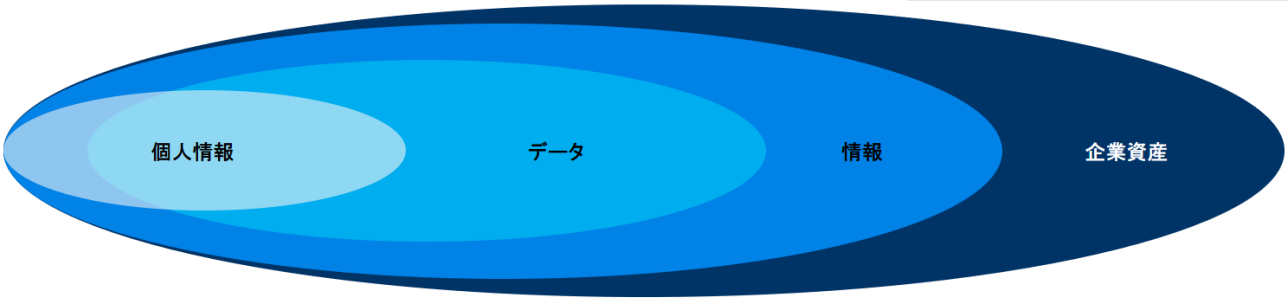


図 2：企業資産の部分集合となるデータおよび情報

1.5 データマネージメント、データコンプライアンスおよび情報セキュリティの各テーマ分野の連携

データおよび情報の取扱いの基本的側面は、データマネージメント、データコンプライアンスおよび情報セキュリティの各テーマ分野の管轄である。

データマネージメントは、透明性を与えデータの利用を可能にする。

- **データマネージメント**は、Mercedes-Benz Group の貴重な資源であるデータの利用と共有について、国際的な指針および最低基準（ミニマムスタンダード）を定める。その際に重要となるのが、データのライフサイクル、データの透明性、データ可用性、また Mercedes-Benz Group にとって効果的で価値を生み出すデータ利用を可能に

[3] デジタル形式の例：電子的に保存されたデータファイル。
物理的形式の例：書類、プロトタイプ

するための、戦略的、組織的および概念的な枠組みを説明することである。

- **データコンプライアンス**はグループ全体に必要な対策とプロセスを定義し、法令を遵守した責任あるデータ（個人情報またはその他のデータ）の取扱いを保証する。重要な項目となるデータ保護（情報保護）では、個人の基本的権利である個人情報の保護を扱う。情報保護は、情報セキュリティの技術的かつ組織的対策を支援する。
- **情報セキュリティ**は、リスクに基づく情報保護のための規則、対策、組織およびプロセスを定義する。リスクを可視化し、それに基づく対策を実施し、その効果を検査する。情報セキュリティは、情報に加えて安全性と企業資産を保護するための重要な要素を管理する。これには特に情報媒体として機能するもの、例えばインフラストラクチャー（サーバー、コンピュータなど）または開発要素（プロトタイプ、デザインモデルなど）が該当する。

データコンプライアンスは、法律に準拠した責任あるデータの取扱いを保証する。

情報セキュリティは、情報の安全性を管理する。

図 3：データおよび情報の取扱いに関連するテーマ分野

情報セキュリティの保護対象に共通する重要項目が以下である：

- **機密性** – 業務上必要な者だけが業務範囲内で特定のデータおよび情報にアクセスすることを保証する
- **完全性** – データおよび情報の正当性と完全性、ならびにそれらの適切な処理を保証する
- **可用性** – 権限のあるユーザー *（第 1.6.1 章を参照）*が必要なデータおよび情報と、適切な IT インフラストラクチャー、IT サービスへ常時アクセスできることを保証する

情報セキュリティには、以下の 3 つの保護対象がある：

- 機密性
- 完全性
- 可用性

以下の項目も十分に考慮すること。

- **信頼性** – データおよび情報が信頼できるものであること。すなわち情報が本物で、証明可能であり、なおかつデータおよび情報の転送が追跡可能であることを保証する。
- **追跡可能性** – ユーザーの行動が追跡可能であることを保証する。
- **否認防止** – ある事象、または行為およびその実行者を証明する手段を保証する（例えば電子署名を使用するなどして、異議を唱えられないようにする）
- **真正性** – ある人物が申告する身元または資源（例：、アプリケーション、プロセス、IT システムなど）が事実通りであることを保証する。
- **耐久性（復元力）** – 内部または外部で予期せぬ障害が発生しても、可能な限り (IT) システムがサービスを提供し、正常なシステム稼働を維持することを保証する。

以下の項目も十分に考慮すること。
- 信頼性
- 追跡可能性
- 否認防止
- 真正性
- 耐久性

1.6 役割と責任

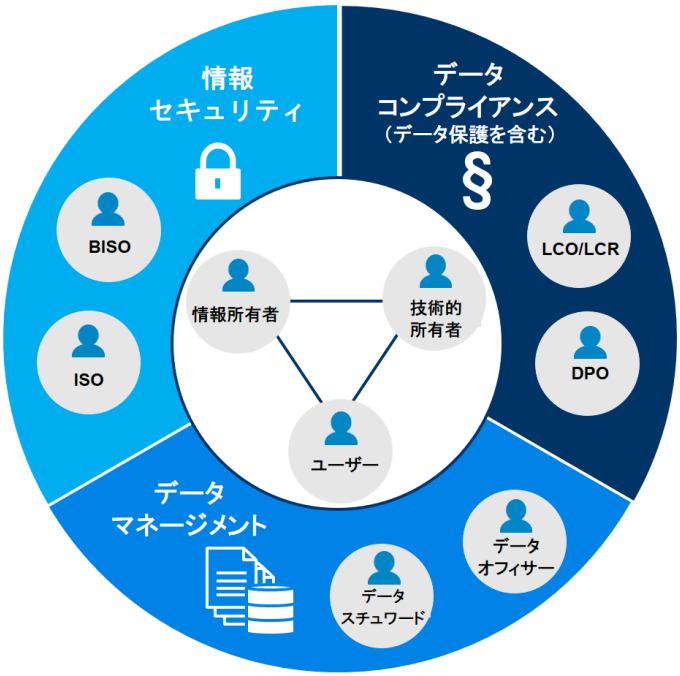


図 4：総合的役割およびテーマ分野別役割

1.6.1 役割

本規程で扱う主要な役割は以下の通りである：

- **ユーザー**とは、Mercedes-Benz Group または第三者のデータや情報にアクセスする、もしくはデータ処理を行う全従業員（または第三者も含む）を指す。ユーザーは、本規程の規則に従ってデータおよび情報を利用する責任を負う。
- **情報所有者**は、責任範囲で作成、発生、利用または管理されたデータと情報に関して責任を負う。これは社外パートナー、エンドユーザーまたは車両使用者から Mercedes-Benz Group へ委託されたデータと情報にも適用される。
- **技術的所有者**は、情報所有者の要望に応じてデータと情報を管理する。第三者が運用者となる場合もある。

本規程の主たる役割：
- ユーザー
- 情報所有者
- 技術的所有者

上記の役割は、以下の各テーマ分野の役割から助言とサポートを受ける：

データマネージメント:

- **データスチュワード**とは、情報所有者の責任範囲の内容に関連した職務を実施可能にするための専門家である。
- **データオフィサー**は担当のデータドメインにおけるデータ戦略および指針を設置する権限を持つ。データスチュワードおよびデータオフィサーは、Mercedes-Benz Group 内でのデータの利用および共有を要求する。これについてはチーフデータオフィサー[4]の要望を考慮し、それぞれの情報所有者と協力して行われる。

データコンプライアンス(データ保護を含む):

- **現地コンプライアンス責任者 (LCO) /現地コンプライアンス担当 (LCR)** には、例えばデータコンプライアンス対策を実行する際に、現地のマネージメントをサポートする役割がある。
- **データ保護責任者 (DPO)** には情報保護責任者としての法的な役割があり、個人情報の保護に関連するあらゆる問題に対して、規則に従って早い段階で関与する。

情報セキュリティ:

- **ビジネス情報セキュリティ責任者 (BISO)** は透明性を確保する責任を担い、自らの事業範囲における情報セキュリティ要件の実施に関する複合的な役割を果たす。
- **情報セキュリティ責任者 (ISO)** は、情報セキュリティおよびサイバーセキュリティの確立を目的として、責任範囲の専門部署が情報セキュリティ職務の計画、調整、管理を行う手助けをする。

以下の役割が各自のテーマ分野で助言やサポートを提供する:

- データスチュワード
- データオフィサー
- 現地コンプライアンス責任者/ 担当
- データ保護責任者
- ビジネス情報セキュリティ責任者
- 情報セキュリティ責任者。

1.6.2 責任者

テーマ分野の責任は、以下のように分類されている:

- データマネージメントに関するガバナンスは、**デジタルコンプライアンスおよびプログラム**部門が責任を担う。
- **コーポレートデータ保護 (CDP) によるデータコンプライアンスおよびデータ保護は、コーポレートデータ保護 (CDP)** 部門が責任を担う。
- 情報セキュリティは**ガバナンス情報セキュリティ (GIS)** が責任を担う。情報セキュリティの目標を達成するために(第 4.1 章を参照)、**GIS** は特に以下の役割を担う:
  - Mercedes-Benz Group 内の情報セキュリティ組織を確立する
  - 情報セキュリティリスクの取扱いに関して、規制政策となる構造を用意する
  - 規制の枠組みを作り、同時に適用される規則を発効させる(規程が最上位)
  - 情報セキュリティの監視および評価を行う

個別のテーマ分野については、以下の専門部署が責任を負う:

- デジタルコンプライアンスおよびプログラム
- コーポレートデータ保護
- ガバナンス情報セキュリティ

[4] チーフデータオフィサーに関する詳細は*ロールハンドブック*を参照。

意思決定およびエスカレーション機関である**データガバナンス委員会**は、データガバナンスに関連するテーマについて部門や役職を超えた採決を行う。本規程の改定や実施に取り組み、その管理を行う。また、データマネージメント、データコンプライアンス（情報保護を含む）、情報セキュリティに関するグループ会社全体の中核テーマに対しても同様に実施する。

データガバナンス委員会 (Data Governance Board) は、本規程のテーマ分野に関する意思決定およびエスカレーション機関である。

個人の役割および責任範囲については、同時に適用される規則*ロールハンドブック*に詳細が記載されている。テーマ分野に関する連絡先一覧は、*同時に適用される規則と、「グローバルデータおよび情報規程に関する連絡先」を参照*すること。

2 データマネージメント

2.1 データのライフサイクル

データライフサイクル管理の目的は、データのライフサイクルにおける段階に基づいて、それに関連する責任者を指名し、責任を担う役割（*第 1.6.1 章を参照*）を割り当てることにある。

データライフサイクル管理ではさまざまな段階について説明し、責任および役割を定義する。

図 5 に示す通り、データはそのライフサイクルにおいて複数の段階を経ることになる：

- 作成
- 利用
- アーカイブ
- 削除

図 5：データのライフサイクル

データオフィサーによるデータ戦略および指針に基づき、情報所有者は法的要件、契約上の要件、グループ社内の要件を考慮した上で、責任範囲の業務プロセスでの実践を主導する。

データ戦略および指針に加え、グループ社内の要件についても考慮する必要がある。

さらに、同時に適用される規則 *データマネージメントガイドライン*に記載されている内容も適用される。

2.1.1 発生 (Creation)

データは、生成、調査収集、社内または社外への委託によって発生する。

Mercedes-Benz Group における透明性を確保するためには、責任を担う情報所有者がデータの発生段階の初期評価を行う必要がある。最低限以下の項目が含まれる：

透明性を確保するために、データの説明が必要となる。

- 情報を分類する（*第 4.2.1 章を参照*）、ラベル付けを含む
- 最低限の情報を説明する（*第 2.3.1 章*）
- データの重要性を規定する（*第 2.3.2 章*）
- 必要に応じて目録を作成する（*第 2.3.3 章*）

データが利用段階にある間は、以上を最新の状態に保つこと。個人情報が存在する場合は、*EU データ保護規則*、*A 17* の適用範囲に該当するデータであるか確認する。適用範囲に該当する場合、取扱い活動の記録 (RoPA) にある文書化の要件を参照すること。

情報所有者はデータのアーカイブまたは削除について、法的要件および業務上の要件に基づいて精査し、必要に応じて決定する責任を負う。

2.1.2 利用 (Usage)

利用段階とは、提供されたデータにアクセスできる利用可能な期間を指す。利用段階中にデータを保存することを保管という。

利用時の責任（*第 2.2 章*を参照）は、データ発生段階で情報所有者が記載したデータの特徴に応じる。

利用時は情報所有者の指示を遵守すること。

さらに情報所有者 は、データの品質が適切であるよう配慮し（*第 2.4* 章を参照）、また必要に応じて品質評価を実施する責任を負う。ユーザーは、データ利用時に発見した品質の欠陥について情報所有者に報告する。

実施可能かつ経済的にも適正である場合に限り、ユーザーはデータをソースから取得するか、または直接ソースシステムのデータで作業する必要がある。

データの結合、蓄積、または分析によって新規データが発生すると（*第 2.2.2 章*を参照）、新たなライフサイクルが開始する。

2.1.3 アーカイブ (Archiving)

法的要件、契約上の要件、またはグループ社内の要件により、データの削除前に編集できない読み取り専用の形式でアーカイブする必要が生じる場合がある。アクセス権限は、アーカイブへのアクセスが必要となる者に限られる。そのためには、適切なアーカイブシステムを使用しなければならない（*データマネージメントガイドライン*を参照）。

データは以下に基づき削除前にアーカイブできる：
- 法的要件
- 契約上の要件
- グループ社内の要件

管理職[5]は各自の責任範囲において、法的要件、契約上の要件、またはグループ社内の要件に従って生成あるいは使用されたデータのアーカイブに対する責任を負う。適切なアプリケーションの用意および技術的なアーカイブ規則の監視は、管理職と合意の上で技術的所有者（*データマネージメントガイドライン*を参照）が行う。Mercedes-Benz Group にとって歴史的意義のあるデータについては、さらに*法人方針資料保管方針*、*A 7* が適用される。

2.1.4 削除 (Deletion)

データは削除の段階で完全に破棄され、Mercedes-Benz Group では使用不可能となる。

---

[5] アーカイブおよび削除を実施する責任は、そのデータを担当する各管理職が負う。データを受領した部門の情報所有者または管理職を指す（第 2.2.1 章）。

個人情報 は、目的に従ってデータを処理する必要がある期間のみ保管またはアーカイブが認められる。すなわち個人情報は、処理の目的が終了した時または何らかの理由で消滅した場合、保管義務もしくは証明義務が引き続き存在する場合を除き、すみやかに削除または匿名化されなければならない[6]。個人情報を処理する IT アプリケーションは、自動または手動による削除サイクルを備えていなければならない。

個人情報は、処理の目的が終了した時点で削除または匿名化されなければならない。

管理職は、各自の責任範囲においてデータが規則通り削除される責任を負う。主に削除を技術的に実行する技術的所有者 の合意の上で削除を行う。

管理職は、削除が規則通り実施される責任を負う。

E メールサーバー、ネットワークドライブ、SharePoint などに保存された共通のデータ削除期限については、[7]データの削除に関する統一プロセスも含めて *データマネージメントガイドライン*に記載されている。

ユーザーのみアクセス可能で削除サイクルが設定されていない場所またはデータキャリア（ローカルや外部ハードディスク）にデータが保存されている場合、ユーザーが利用段階またはアーカイブ段階が終了したデータの削除、もしくはローカルデータの削除を行わなければならない。

2.2 データ所有権

データ所有権の目的は、持続可能で、効率的かつ効果的なデータの取扱いのために、責任の所在を明らかにしておくことにある。

データ所有権はデータの取扱いに関する責任を明確にする。

「所有権」という用語は、データマネージメントにおける重要な役割、特にデータを利用可能な状態にする、共有する（データシェアリング）、データを慎重に保管し保護するという責任を意味する。「財産」または「所有」を意味するものではない。

2.2.1 データ移転に関する責任

規則に従ったデータ転送とその後の利用のため、情報所有者は転送前に最低限の情報（*第 2.3.1 章*を参照）を各自の責任範囲（A 部門）にあるデータについて記載し、受領側の職務部門（B 部門）に提供する責任がある（*図 6 参照*）。

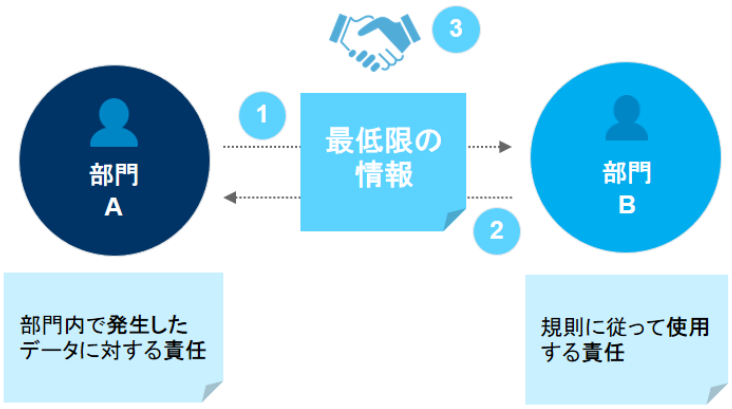
受領側の B 部門のユーザーは、データの利用前に最低限の情報と部門固有の内部および外部要件を把握しておく責任がある。ユーザーは各自の権限の範囲内で適切に利用する責任がある。

受領側の部門のユーザーは、各自の責任について前もって通知を受ける。

提供側の A 部門による転送と受領側の B 部門による利用をもって、最低限の情報および要件が了承されたものとする。

6 そのような場合は、処理の新たな目的が証明となる。

7 これに関連して、*IT 端末およびカメラに関する規程、A 32* も重要である。



1 A部門は最低限の情報を説明し、変更点についてBに通知する(「情報通知義務」)。

2 B部門は最低限の情報および部門別要件に応じて、規則に従ってデータを取り扱う(「情報取得義務」)。

3 Aによるデータ移転とBによるデータ使用をもって、同意したとみなされる。

図6:データ移転に関する責任

第三者に対するデータ転送では、さらにデータクリアリングプロセスの要件を適用する(*第3.1.5章*)。

2.2.2 データ結合に関する責任

さまざまな責任範囲にあるデータの統合または外部データとの結合によって、新たなデータが発生することがある。そのようなデータを業務プロセスで利用する場合、新規データまたは結合データを作成した部門の管理職が情報所有者となる。

データの統合または外部データとの結合によって、新たなデータが発生することがある。

情報所有者はデータソースの既存の制限を考慮および遵守し、必要があれば最低限の情報に補足するか、または説明を新たに記載し直す責任も負う(*第2.1.1章*)。

データ結合では、さらにデータ分析のためのコンプライアンスフレームワークの要件も適用される(*第3.1.4章*)。

2.3 データの透明性

データの透明性によって、データの状態、来歴、利用に関して透明性が確保され、データ駆動型ビジネスモデルや効率的な作業プロセスが可能となる。

データの透明性とは、データの状態、来歴、利用に関する透明性を指す。

以下の要件は、グループ会社のデータ、共同で利用されるデータ(部門を超えた利用、または Mercedes-Benz Group の外部企業との提携など)、および第三者のデータに適用される。

実施に関する詳細な指針およびヘルプは、*データマネージメントガイドライン*に記載されている。

2.3.1 データ移転のための最低限の情報

転送時、データには最低限の情報を記載しておく必要がある。情報所有者は、データの転送の前提となる以下の情報を適切な方法で記録または識別し、データ移転時に提供する責任を負う:

- 情報の分類（*第 4.2.1 章*）
- アーカイブ
- 削除
- その他の情報（例：作成時の意図、法的要件、契約要件、社内要件など）。転送および利用にあたって重要となる場合

データの利用時には、このような最低限の情報を参照しなければならない。

最低限の情報を記録しラベル付けするための移行期間が適用される。これについては *Guide Data Management（データマネージメントガイドライン）*を参照すること。

2.3.2 データの重要性

Mercedes-Benz Group にとって特に重要なデータを情報資産という。データの改変、紛失、誤用により、損害のリスクが生じる。

特に重要なデータを情報資産という。

データの重要性を決定し適切に取り扱うため、情報所有者は各自の責任範囲で、Mercedes-Benz Group にとってのデータ価値と保護の必要性を考慮して等級分けを行う。

データの重要性を決定するのは情報所有者の責任である。

価値はそれぞれの文脈に応じて発生し、[8]データライフサイクルの過程で変化することがある。

[8] 「70563」という数字は、文脈がなければ価値を持たない。しかし、リース契約書に記載されたドイツの顧客データの「郵便番号」であれば、Mercedes-Benz Group に価値をもたらすことがある。

重要性を決定する指針として、表 1 に記載の基準が役立つ:

基準	説明
社外の市場価値	市場における情報資産の費用または価値
展望	情報資産の利用潜在性
消費者	消費者の数または業務プロセスでの使用
保護の必要性	情報の分類に応じる
その他の基準	例えば法的要件、法的重要性、意思決定への重要性、監査への重要性など

表 1 : 情報資産の重要性を判断する基準

各データオフィサーは、これに基づいて情報資産の概要を各自の責任範囲で作成し、データ戦略で考慮する必要がある。

2.3.3 情報資産台帳

情報資産台帳はデータを見つけやすくし、情報資産の透明性を高める。

情報資産台帳は、Mercedes-Benz Group のあらゆる情報資産に共通の目録である。データを見つけやすくし、データの透明性を高めることが目的である。

ここではデータの追跡可能性 (Traceability) も重要となる。この用語には、情報資産の来歴、利用、転送(発生から、消費ユーザー、プロセス、またはシステムに至るまで)に関する情報が含まれる。

情報所有者は、各自の職務部門で発生した情報資産を特定し、情報資産台帳に記録して最新の状態に保たれなければならない。データスチュワードが設置されている場合は、情報所有者を支援する。

目録作成の要件を実施するための移行期間が適用される。これについては *Guide Data Management (データマネージメントガイドライン)* を参照すること。

2.3.4 データモデル

データモデルはデータの要件および関連を示す。

データモデルの目的は、データ図のモデルを用いて、複雑な関係性や関連性を総合的な一覧図で分かりやすく示すことである。

情報所有者は、データモデルを適切に記録する責任がある。すでに確立されている業界基準または Mercedes-Benz Group の専門要件に基づいて、社内および第三者と効率よくデータを共有または交換、もしくは結合するために行う。

責任範囲または業務プロセスのデータは、その関係性を図を用いて記録される。データモデル図では、マスターデータにも[9] 特別な役割が与えられることがある。

[9] マスターデータとは、例えば顧客番号、部品番号、コストセンター、工場番号、法人名称、FIN(車両識別番号)などを指す。

2.4 データ品質

データ品質はデータの有用性を決定づける。

データ品質の目的は、データの信頼性に関する基準を定めることにある。データがどの程度事実に即しているかを示し、データの有用性を大幅に決定する。優れたデータ品質は、適切なプロセス、分析などの数学的手法、最適な決定、高い効率性を実現するために重要となる基本条件である。また、信頼できる製品やサービスの基本でもある。データの発生段階からこのような視点を持ち、考慮しなければならない。

形式、構造、内容がデータを構成し、いずれもデータの品質に影響を及ぼす。情報所有者はデータ品質を判断するために、適切で、共通定義された、一貫性のある、目的に適った基準を策定する必要がある。そうした基準は、データ品質に関して測定可能で信頼できる意見を述べるために役立つ。基本的な基準は、適用事例や使用形態に応じて、また考慮する段階に応じて異なる可能性がある。

表 2 は、Mercedes-Benz Group にとって重要なデータ品質基準を示す。

基準	説明
最新性 (Timeliness)	データはすべて最新の状態に保たれている。
一意性 (Uniqueness/ Deduplication)	データはすべて明確に解釈できる。データに重複がない。
正確性 (Accuracy)	データはすべて要件通りに正確である。
妥当性 (Validity)	すべてのデータが規定された共通の適用範囲に対応している。
正当性 (Integrity)	データレコードはどれも矛盾していない。完全性、正確性、一貫性を備えている。
一貫性 (Consistency)	あるデータが、他のデータに対して矛盾することがない。
合理性/関連性 (Reasonability)	データの概念や構造は、情報の受領側の想定と一致していなければならない。
完全性 (Completeness)	データには必要な属性がすべて含まれている。

表 2 : 選別されたデータ品質基準の定義

基準を測定するためには、追跡可能な計算、公式または説明に基づき、規定の要件をどの程度満たしているか確認できなければならない。基準の測定とふさわしい品質を追求することは、継続するプロセスである。

極端な労力をかけなければ上記のデータ品質基準を満たすことができない場合、データオフィサーとの合意の上で、上記の基準から複数を組み合わせて 1 つの基準にまとめた追加の基準を定義し記録する。

データ品質の評価、遵守、改善のために講じる対策は、技術的および経済的に可能であれば、必ず本来のデータソースに対して実施すること。

情報所有者は、各自の責任範囲に該当する基準に従い、適切なデータ品質規則を定義する。品質基準の決定、具体的な基準の設定、持続的な実施についても、同様に情報所有者が責任を負う。データオフィサーは、各情報所有者にデータ品質対策を要求することができる。

情報所有者は、最適な品質基準を定義し策定する責任を負う。

上記は主に、重要性検査（第 *2.3.2 章*を参照）に基づいて重要性が高いと判断された情報資産について考慮される。

情報所有者は、必要に応じて技術的所有者の合意の上、データ品質を確保する適切なプロセスまたはふさわしいシステムを提供する必要がある。職務詳細は *データマネージメントガイドライン*に記載されている。

品質に関する問題は、情報所有者に報告しなければならない。

3 データコンプライアンス（データ保護を含む）

Mercedes-Benz Group は、法律を遵守し、倫理的に正しく責任を持ってデータ全体を取扱うという個人情報の保護が、データガバナンス全体に不可欠な要素であると理解している。

Mercedes-Benz Group の情報保護文化は、*EU データ保護規則*、*A 17* と合わせて、下記データコンプライアンスの国際基準に記されている通りである。

Mercedes-Benz Group 内での一貫したデータ保護レベルの基本となるのは、データコンプライアンスの国際基準である。

「グループユニット」という用語には、グループ会社だけでなくメルセデス本社も含まれる。

3.1 データコンプライアンスの国際基準

下記にあるデータコンプライアンスの国際基準は、国際的に承認されている情報保護の基本原則に準拠し、Mercedes-Benz Group 全体で一貫した情報保護レベルを実現する基本となるものである。これは既存の事業活動におけるデータの取扱いと、データ駆動型の新規ビジネスモデルを担当開発する際に適用される。

Mercedes-Benz Group は、情報保護に関する各国の規制に多様性があり、異なる社会的期待があることを考慮している。そのような多様性を尊重すべくデータコンプライアンスの国際基準は、現地の情報保護法を遵守しデータコンプライアンスマネージメントシステム（データ CMS）をグループ全体に適用した上で、法律に準拠した持続可能なデータの取扱いを保証するためにグループ全体の統一的な枠組みを定める。その際、国際基準は最低限の水準（ミニマムスタンダード）として理解し、必要に応じて各グループユニットは法律拘束力のある現地の規則によってさらに改定を加えてもよい。

データコンプライアンスの国際基準は、データ CMS とともに法律に準拠した持続可能なデータの取扱いを保証する。

Mercedes-Benz Group の全会社が、国内の情報保護法を厳格に遵守すること。法的義務が国際基準に相矛盾する場合は *第 5* 章を参照すること。

データコンプライアンスの国際基準は個人情報の自動処理、すなわちアナログまたはデジタル技術設備（PC、スマートフォン、監視システム、コネクテッドカーアプリケーション、記録デバイスなど）による処理にも適用される。さらに個人情報の非自動処理にも同基準が適用される。個

人の特徴に基づいてデータが構造的に分類されており、個人の特定が可能な場合は、特に紙媒体や書類形式の処理にも該当する。紙媒体の書類に個人情報が偶然含まれているが、個人を特定できない場合には、適用範囲に該当しない。ドイツ国内においては、処理や収集の種類または分析の可否に関わらず、この基準は全従業員のデータにも適用される。

3.1.1 Mercedes-Benz のデータ取扱いに関するビジョンの原則

Mercedes-Benz のデータ取扱いに関するビジョン（「Mercedes-Benz Data Vision」）は *第 1.3 章* に記載があるが、同時にデータコンプライアンス戦略についても示している。その 7 つの原則は、Mercedes-Benz Group における一貫した情報保護レベルの基本を形成するものである。それらは従業員一人ひとりの日常業務の基本となるものであり、データコンプライアンスの国際基準において下記のように具体化される：

Mercedes-Benz のデータ取扱いに関するビジョンの原則は、データコンプライアンスの国際基準の中でより具体的に述べられている。

事業機会
Mercedes-Benz Group の従業員は、顧客、車両および従業員のデータを責任を持って利用し、Mercedes-Benz Group の事業機会および利益が見込める成長分野の開拓と、社内手続きの最適化を図る。データとは、Mercedes-Benz Group と株主にとって持続的な付加価値を生み出す、保護に値する貴重な資産である。また、将来のデータベース型ビジネスモデルの基本となる。

責任あるデータの利用によって、新たな事業機会を開拓する。

顧客のための付加価値
データを評価するにあたって、Mercedes-Benz Group の従業員は顧客にとって直接的な利益を生み出すよう務める。そうした利益に含まれるものには、顧客がデジタル環境に滞りなくアクセスでき、Mercedes-Benz Group のみまたはサードパーティプロバイダーが提供するシステムを統合することで、快適性の向上、新しい機能、操作性の向上が体験できることなどがある。その際、顧客の期待や好みが地域によって異なることを考慮する。

顧客利益に相反する事業機会を実現させるために、データを利用することは許されない。顧客は Mercedes-Benz Group に対して革新的なサービスを期待すると同時に、個人情報が責任を持って取扱われることを望んでいる。車両の安全性に対する顧客の極めて高度な要求は、デジタルトランスフォーメーションの一連の流れの中で、ネットワーク化された車両データの安全性とその保護にまで広がっている。

データを評価するにあたって、最重要となるのが顧客利益である。

データ品質
Mercedes-Benz Group の従業員は、あらゆる技術的および組織的対策を適切に講じてデータの完全性、正確性および最新性を保証することにより、自ら処理したデータの品質を確保する。高品質の収集データのみが顧客および従業員に付加価値をもたらし、Mercedes-Benz Group 内で職務および組織の枠組みを超えたデータの利用を可能にする（*第 2.4 章*）。

高品質の収集データのみが、顧客および Mercedes-Benz Group にとって付加価値をもたらす。

透明性
Mercedes-Benz Group は、個人情報の取扱いに透明性を求める声が、顧客と従業員の間で高まっていることを認識している。そのため顧客と従

業員に対しては、データ責任者の身元、データ処理の目的、また必要に応じてその他グループ会社や第三者もしくは第三者カテゴリーへのデータ移転が行われることが適切に通知されなくてはならない。社内でも既存データに関する透明性を確保する必要がある。利用可能なデータを把握することでのみ、法的要件を確実に遵守した上で、データを体系的に評価することが可能になるからである（*第 2.4 章*）。

顧客および従業員は、常に自らの個人情報の処理について照会することができる。照会は、各会社に直接問い合わせられるようにしなければならない。照会内容への回答が顧客または従業員から見て十分でない場合、コーポレートデータ保護責任者に問い合わせることができる。照会には、適切な期間に回答すること。

顧客および従業員は、データ処理について適切に通知されなければならない。

選択の可能性
会社においては、顧客と従業員が個人情報の利用について事前に同意または後から同意を撤回することで、個人情報の利用を自ら管理できるようにする必要がある。ただし、法律または契約によってデータ処理の必要性が定められている場合には適用されない。選択の可能性を保証するために、分かりやすい技術的措置を提供する必要がある。そのような措置は高度なユーザーフレンドリーのための基本的前提であり、Mercedes-Benz Group によるデータ利用に対する信頼性を高めるからである。

技術的措置を講じることで、顧客と従業員が自らの個人情報の利用を管理できるようにしなければならない。

データの安全性
グループ共通のデータの安全性に関する対策は、顧客や従業員、ビジネスパートナーが Mercedes-Benz Group を信頼し、個人情報を提供するための基礎を形成するものである。そのため Mercedes-Benz Group では、国際的に統一された高い情報セキュリティ基準を定める（*第 4 章*）。

個人情報は責任を持って取り扱い、適切な技術的および組織的措置を講じて、不正アクセスや不適切な処理または譲渡、および過失による喪失、変更、破壊から保護する必要がある。

情報セキュリティの技術的および組織的措置は、個人情報の保護も対象となる。

会社はデータ処理に新たな手法（特に新たな IT システム）を導入する前に、個人情報保護のための技術的および組織的な対策を定義し、実施する（*第 3.1.3 章*）。それらの対策は、最新技術、処理のリスクおよび情報保護の必要性（情報の分類によって決定する）が考慮されたものでなければならない。

データ倫理
Mercedes-Benz Group の従業員は、企業価値（*インテグリティ規程 (IC)* に定義されている）および規程ならびに法律に準拠し、責任を持ってデータを取扱う必要がある。データを収集および処理するにあたっては、この国際基準に加え *インテグリティ規程 (IC)* 、*EU データ保護規則*、*A 17* および拘束力のある法的要件を厳格に遵守すること。

企業資産、規程、法律に常に準拠して個人情報を処理する。

Mercedes-Benz Group 内のデータに対する責任の重要な要素に、包括的なデータ CMS（*第 3.3* 章を参照）がある。これは情報保護を遵守するためのグループ全体での対策、プロセス、システムを統合したものである。

3.1.2 委託処理

全般

委託者の名前および指示に基づき、受託業者がサービス提供者となり個人情報を処理する場合、これを委託処理という。その場合、社外の受託者のみならず Mercedes-Benz Group 内のグループ会社間でも、委託処理の合意を締結する必要がある。データ処理が正しく実施されることに対するすべての責任は委託会社が負う。

委託処理は、契約で規定する必要がある。

委託の要件

依頼時には以下の規則を遵守すること。委託を行う専門部署は受託業者による履行を保障しなければならない。

- 受託業者は、要求される技術的および組織的な情報保護対策を講じることを保証する能力のある業者でなければならない。
- コーポレートデータ保護責任者が用意した契約基準が遵守されなければならない。
- 委任は書面または電子形式で行うこと。データ処理に関する指示、および委託側と受託側の責任者名を記録すること。

委託者はデータ処理の開始前に適切な精査を行い、受託業者が前述の義務を果たしていることを確認しておく必要がある。加えて CDP（コーポレートデータ保護）が設ける規則（例：ソフトウェアツール、評価の実施に関する指示など）も考慮すること。受託業者は、証明書をもって情報保護要件の遵守を証明することができる。データ処理のリスクに応じて、契約期間中は定期的な検査を繰り返し行うこと。

委託者は、情報保護要件が受託業者によって遵守されているか確認すること。

契約期間中に受託業者に対して、契約で合意した契約対象とは異なるあるいは契約を超えた指示を与える場合、委託側は書面にて指示を出し記録をすること。

グループ社内での委託処理規則

グループ会社間で委託処理契約を締結する場合、必ず書面または電子形式で記録すること。加えて Mercedes-Benz Group の規則（例：契約管理ツール、基本協定など）も考慮すること。

委託処理は、グループ社内であっても契約書で規定する必要がある。

個人情報の処理については、受託者が事前に委託者の承認を得ている場合に限り、他のグループ会社または第三者（「再委託業者」）に対して委託（再委託）することが認められる。承認が許されるのは、受託者が再委託業者に対し、情報保護および情報セキュリティに関して受託者と同等の義務を（契約により、または同等の法的要件により）課す場合に限られる。

受託者は、再委託業者が情報保護に関する法的義務または契約上合意した義務を遵守するよう、適切に支援しなければならない。受託者はさらに、委託者（存在する場合はその上の委託者）に対し、データ主体による要求、申請、または苦情をただちに報告し、情報保護に関する事案（*第 3.1.6* 章を参照）について情報を提供する義務を負う。

3.1.3 技術設計による情報保護(「プライバシーバイデザイン」)

個人情報の処理を必要とする IT システムまたはプロセスを計画する際には、情報所有者が最適な技術的および組織的対策を採用し、上記 Mercedes-Benz のデータ取扱いに関するビジョンの原則を効果的に実施しなければならない。それには最新技術、利用データの種類と範囲、処理状況と目的、データ主体に損害が及ぶ可能性とその可能性の高さについて考慮する必要がある。

システムおよびプロセスの計画段階ですでに情報保護を考慮しておく必要がある。

3.1.4 データ分析のためのコンプライアンスフレームワーク

*データ分析のためのコンプライアンスフレームワーク*は、適用範囲に記載されている Mercedes-Benz Group の全従業員への適用が義務付けられる。フレームワークに定められている規則は、すべての関連法域を考慮した上で、法律に準拠したデータ分析の実施を保証する(特に 情報保護、製品安全性/ 製造物責任、独占禁止法、銀行法)。難しい事例では、その都度必ず LCO/ LCR が関与し、必要に応じてデータコンプライアンス・コンピテンスセンターに相談する。

データ分析のためのコンプライアンスフレームワークは、法律に準拠したデータ分析の実施を保証するものである。

3.1.5 データクリアリングプロセス

Mercedes-Benz Group からビジネスパートナーへのデータ移転、または場合によってデータが収益化される前に、データクリアリングオフィスによる監査および承認を受ける必要がある。データクリアリングプロセスは、義務付けられているグループユニットおよびデータ移転時に必須のものである。データクリアリングプロセスの一環として、データコンプライアンス・コンピテンスセンターはデータ移転の合法性および各ビジネスパートナーのインテグリティを検査する。データクリアリングプロセスの目的は、ビジネスパートナーへのデータ移転に関する透明性を高め、潜在的なデータリスクを最小化にすることにある。

データクリアリングプロセスはビジネスパートナーへのデータ移転に関する透明性を確保し、リスクを最小化する。

データの販売については、*販売パートナーとの事業協力に関する規程、C 146* を適用してはならない。

3.1.6 情報保護に関する事案の報告

Mercedes-Benz Group ではあらゆる情報セキュリティ事案について、24 時間利用できる集約型の報告プロセスが確立されている。これを情報セキュリティインシデント管理プロセスという。従業員もまた、このプロセスによってあらゆる情報セキュリティ事案、すなわち情報保護違反の疑いを内部通報する必要がある。個人情報保護違反は、不法な削除や変更、個人情報の不正公開や利用につながるデータの安全性を侵害する行為である。

情報セキュリティインシデント管理プロセスには、情報保護に関する事案も報告する必要がある。

報告は Cyber Intelligence & Response Center に以下の方法で行う。電話番号:+49 711 17-76758 本部 E メールアドレス:
cyber.security@mercedes-benz.com

情報セキュリティインシデント管理プロセスで報告された情報保護事案は、CDP(コーポレートデータ保護)へ転送される。EU 一般データ保護規則 (EU-GDPR) の適用範囲となるユニットでは CDP(コーポレートデータ保護)がその後も引き続き対応し、特に情報保護違反を確定するための初期

評価を行う。加えて、現地で事実調査を行う現地のインシデントサポート（通常は LCO/ LCR）が関与する。場合によりデータ主体の権利と自由に対する不利益の可能性を考慮し、必要なリスク分析を行った後、法規の期限である 72 時間以内に監督当局への連絡とデータ主体への報告を行う必要性があるかどうかについて、CDP が経営陣メンバーに対策を推奨することが本プロセスでは想定されている。

EU-GDPR の適用範囲外のユニットでは、現地のインシデントサポート（通例は LCO/ LCR）が現地の情報保護法の要件に従って引き続き対応する。本プロセスは、インシデントサポートおよび現地経営陣メンバー間で、法規の期限内に必要な監督当局およびデータ主体に報告を行うかどうか採決を取ることを想定している。CDP はいつでも支援のために関与することができる。CDP は調査結果を記録のために提供しなければならない。

現地のグループユニットは事案の解明を支援し、そのために必要な資源を提供しなければならない。現地のグループユニットは、事案の影響を最小化し今後の事件リスクを低減するために必要な対策を実施する必要がある。調査済みの情報セキュリティ事案の評価から得た知見は、データコンプライアンスマネージメントシステム（データ CMS、*第 3.3* 章参照）に反映される。

3.1.7 情報保護に関するアドバイス

*コーポレートデータ保護*のイントラネットサイトにはデータ保護に関する主な情報が記載されており、従業員はここから情報を得ることができる。このような一般的な情報提供の他、コンプライアンス組織は情報保護に関するあらゆる疑問に回答する。

コンプライアンス組織は、総合的な情報とアドバイスの場を提供している。

情報保護に関する質問を最初に担当するのが LCO および LCR である。現地のコンプライアンス窓口が質問に回答できない場合は、質問をコーポレートデータ保護部門に転送する。

新たな処理作業が確立された場合、または既存の処理作業が根本的に変更された場合、あるいは処理作業の合法性に疑いが生じた場合は、情報保護に関するアドバイスを LCO/ LCR に仰ぐことが全従業員に対して義務付けられている。

それとは別に、全従業員には、情報保護責任者およびコーポレートデータ保護部門に情報保護に関して直接問い合わせる権利がある。

3.2 EU データ保護規則

EU-GDPR に関連するより上位の情報保護要件は、*EU データ保護規則、A 17* で扱う。

EU-GDPR の適用範囲には、*EU データ保護規則、A 17* も適用される。

EU データ保護規則、A 17 は EU-GDPR の適用範囲内で有効であり、個人情報の処理に適用される。

- 所在地が EU[10]域内にあるか、または本規程が適用される国にあるグループ会社
- EU に滞在する人物に商品またはサービスを提供する、またはその行動を監視する EU 域外のグループ会社
- 前述のいずれかに由来するデータを EU 域外のグループ会社が処理する場合

EU データ保護規則、A 17 は EU-GDPR が要求する情報保護レベルを保証し、EU 域外のグループ会社がグループ会社の個人情報を転送するにあたって、拘束力のある規則を策定する。そのため同等の情報保護レベルが存在しない国においても、Mercedes-Benz Group 内であれば境界のないデータ交換が法的に可能になる。

EU データ保護規則、A 17 に従い、個人情報はグループ会社間で転送することができる。

以下の図 7 では、データコンプライアンスの国際基準と比較した *EU データ保護規則 (A 17)* の適用範囲と実効範囲を示す（*第 3.1 章*）:

図 7 : データコンプライアンスの国際基準および EU データ保護規則、A 17 の適用範囲および実効範囲

3.3 データコンプライアンスマネージメントシステム

3.3.1 目標設定および責任

データ CMS の目的は、Mercedes-Benz Group におけるデータ処理活動全体について、情報保護法上有効な規則の遵守を保証することにある。これは情報保護に関する国内法および国際法、特に EU-GDPR の遵守に関連し、データ主体の権利を保証し、Mercedes-Benz Group を不正または安全ではない、非倫理的な個人情報の取扱いによる風評被害や信頼の喪失および物質的損害から保護することにつながる。

データ CMS は、グループ会社におけるデータ保護規則の遵守を保証するために必須となる対策を定義する。

[10] *EU データ保護規則、A 17* に関して、「EU」という語には欧州経済領域 (EEA) 内のすべての国が含まれる。すなわち EU 加盟国の他、ノルウェー、アイスランドおよびリヒテンシュタインが加わる。

データ CMS は、すべてのグループユニットがデータ保護規則を遵守するために必須となる対策と、それに基づき経営陣メンバーおよび従業員に対して発生する義務と職務を定義する。

各グループ会社を運営する経営陣は、情報保護法の遵守する責任（「データ責任者」）とデータコンプライアンスの目的を達成する責任を負う。Mercedes-Benz Group AG、Mercedes-Benz AG、Mercedes-Benz Mobility の経営陣は、データコンプライアンス対策の実施をメインユニットの統括者に委任し、対策の実施について、特にデータ CMS が行う監視を管理する。

グループユニットの経営陣および主要部門の統括者は、データ CMS の要件を現地で実施するために十分な資源を提供し、組織的、人事的および技術的対策を講じて情報保護に準拠した適切な個人情報の処理を保証する必要がある。

データ CMS がグループ会社の経営陣メンバーおよびメインユニットでレベル 3 以上の統括管理職に対して求める要件は、その他の適用規程 *Data CMS requirements for the management（マネージメントのデータ CMS 要件）*に定義されている。

3.3.2 データコンプライアンス対策

*データコンプライアンス対策*では、特定のリスクに的を絞って対処すべくグループユニットに毎年義務付けられる対策が定義されている。対策の実施は義務であり、経営陣メンバーが責任を負い LCO/ LCR が支援を行う。この *対策*はコーポレートデータ保護部門によって毎年更新され、グループ会社およびメインユニットに送付される。

3.3.3 EU-GDPR の実施対策

EU-GDPR の要件を満たすため、規則の適用範囲内でグループユニットに向けて特別な対策を定義する。これは *データコンプライアンス対策*の一部であるため、経営組織メンバーは必ず実施しなければならない。

3.3.4 EU 域外のグループユニットにおける現地の情報保護法の実施対策

EU-GDPR の適用範囲外のグループユニットでは、データコンプライアンスの国際基準（第 3.1 章を参照）が最低限の基準として現地で実施すべき対策を定義する。これは *データコンプライアンス対策*の一部であるため、経営組織メンバーは必ず実施しなければならない。補足として EU に属さない各グループユニットは、現地の情報保護法に基づき法的拘束力のある具体的対策を必要に応じて定める必要がある。すべてのグループ会社には、現地の情報保護法の法的枠組みを精査の上で記録し、変更点をコンプライアンスモニタリングの一環としてコーポレートデータ保護部門に報告することが義務付けられる。万が一新しい情報保護法が国際基準と矛盾する場合は新たな規則がグループ会社に与える具体的影響と、現地プロセスおよび規則に適合させる必要性について詳しく説明しなければならない。

データコンプライアンスの国際基準は最低限の水準（ミニマムスタンダード）を定めたものであり、現地の情報保護法に基づく法的拘束力のある対策によって補足される。

4 情報セキュリティ

4.1 情報セキュリティの目的と要件

情報セキュリティの目的（*第 1.5 章*を参照）を**効果的かつ効率的に実行するため**、情報セキュリティは体系的取り組みとして情報セキュリティマネージメントシステム (ISMS) を採用する。本システムは、**可用性、完全性、機密性**を考慮した情報保護を行うことで、業務プロセスを支援することを目的としている。Mercedes-Benz Group の ISMS は、情報セキュリティに関する国際標準規格 ISO/IEC 27000 に準拠している。

情報セキュリティの目的を達成するためにマネージメントシステム (ISMS) を使用する。

Mercedes-Benz Group の情報セキュリティに関する規則の詳細は、同時に適用される規則*情報セキュリティ規則* (RISE) に記載されている（参照標準：*Organisation der Informationssicherheit（情報セキュリティの組織）*およびポータルコード@RISE）。

RISE が情報セキュリティの詳細を定める。

RISE 規則の**遵守**については、**必ず管理職**および GIS が各自の責任範囲で定期的に**検査する必要がある**。

事業範囲の統括者は、情報セキュリティのプロセスが自国の法的条件に適合していることを確認する必要がある。

Mercedes-Benz Group の情報へのアクセス権を持つまたはアクセスに関して責任がある第三者に対しては、委託を行う専門部署が、Mercedes-Benz の購買および調達プロセスの枠組みの中で契約条項を定めることで、適切な情報セキュリティレベルを保証する必要がある。第三者による契約上の規則の遵守（例：個人情報に関する法的要件など）は、委託を行う専門部署によって適切な範囲で検査する必要がある（参照標準：*下請け業者との関係*）。

4.2 日常業務での情報利用

ユーザー、情報所有者、技術的所有者の職務と責任については RISE で詳細が説明されている。以下の行動指示は、役割がユーザーの従業員に該当する。ここでは、従業員がユーザー役割の日常業務を行う際に、定期的に重要となる典型的な内容について説明する。

RISE には、情報セキュリティのあらゆる役割が説明されている。

4.2.1 分類

企業情報を、各情報の重要性に応じての適切な保護するため、**情報所有者が責任部門の情報分類を行う**（参照標準：*価値の管理*）。

情報の分類では、**機密性に関する**企業情報は以下の**保護段階**のいずれかに分類される：

情報は 4 つの保護段階のいずれかに分類される。

- 一般（*社外公表に関する規程、A 23* を参照）(Public)
- 社外秘 (Internal)
- 秘 (Confidential)
- 極秘 (Secret)

情報が分類されていない場合は、「社外秘」として取り扱う必要がある。企業情報には **Need to know の原則**を適用する。この原則は、情報にアクセスする権利があるのは、仕事の一環としてその情報が必要な者に限ら

分類のない情報は社外秘として取り扱う。

れることを意味する。どのユーザーにも、情報の分類の要件に従った情報の取扱いが義務付けられる（ポータルコード @infoclass を参照）。

秘情報および極秘情報の安全性と保護には、特に高い要件を適用する。その一部を下記の表に示す：

特に秘情報および極秘情報に対しては高い要件を適用する。

プロセス	秘情報	極秘情報
ラベル付け	必ず最初のページ（画面）上に「vertraulich（秘）」の印を押す	必ず各ページ（画面）上に用語「geheim（極秘）」の印を押す
保管	情報媒体は必ず安全に保管しなければならない。	
	情報を破棄する場合は、情報を復元できない状態で処分する。	情報を破棄する場合は、情報を復元できない状態であることが証明可能な方法で処分する。
暗号化	必ず暗号化して伝送する（E メールの送信など）。（例外：特別に保護されたネットワーク）	必ず暗号化して伝送する（E メールの送信など。例外：特別に保護されたネットワーク） 暗号化して保存する
	モバイルデータキャリアでも暗号化する必要がある	
口頭での連絡	口頭による連絡では、決して秘または極秘の情報が権限のない第三者の耳に入らないようにすること。	

表 3：秘情報および極秘情報の安全性および保護に関する要件（一部のみを表示）

4.2.2 情報の保護および転送

ユーザーは職場において、社外秘、秘および極秘の情報を**常に管理下に置き**、画面を**のぞき見ることができない**状態にする必要がある。職場の整理整頓の原則が適用される（「クリーンデスクの原則」、参照標準：*（物理的および環境的セキュリティ）*。監督の行き届かない端末および情報媒体は十分に保護する必要がある。

整理整頓された職場は、情報セキュリティのリスクを最小化する。

例えばノートパソコンの画面は作業場所を離れる際にロックし、機密情報を印刷およびコピーする際は目を離さないようにしなければならない（例：Follow2Print 機能の使用など）。

情報を転送する場合、情報使用者は情報所有者の指示に従って取り扱う、もしくは転送しなければならない。

ユーザーは**情報媒体**を不正なアクセス、濫用または損傷から保護する必要がある。例えば持ち運び時も十分に注意する（参照標準：*価値の管理*）。

例えばノートパソコンや業務関連書類を社外の会場に持参する場合、会議室を退出する際（休憩時間など）にはノートパソコンおよび書類を鍵をかけた状態でしまっておくか、目を離さずにいる必要がある。

4.2.3 情報セキュリティ事案

従業員は 、情報セキュリティ事案および事件・事故、ならびに情報セキュリティの脆弱性を実際に発見するかもしくはそれらが疑われる場合には、ただちに**担当窓口**に報告しなければならない（参照標準：*情報セキュリティ事件・事故への対処*）。

あらゆる情報セキュリティ事象および事件・事故は、報告しなければならない。

現地の通報窓口の他、本部の通報窓口がある
Corporate Security Situation Center (SitCenter 24/7)
+49 (0) 711 17 77377 *SitCenter@Mercedes-Benz.com*

Cyber Intelligence & Response Center (CIRC 24/7)
+49 (0) 711 17 76758 *Cyber.Security@Mercedes-Benz.com*

Mercedes-Benz Group にとっての重要性や被害の可能性は必ずしも一見して認識できるとは限らないため、事件や事故が疑われる事案の**報告**は極めて重要となる。

ノートパソコンの紛失または盗難に遭った場合、例えば保存データにアクセスされることがあると情報セキュリティに影響を及ぼすため、ただちに報告しなければならない。

情報が保管されている鍵のかかった書類棚に引っかき傷を発見した場合は、ピッキングや盗難の疑いがあるため、ただちに通報する必要がある。

例えば USB メモリーが放置されているのを見つけた場合、中に機密の企業情報または悪意のあるソフトウェアが保存されている可能性がある。USB メモリーを接続してはならず、拾得物はただちに報告しなければならない。

4.2.4 パスワードの保護

パスワード（例：Windows 認証、社員ポータルなど）は企業情報の保護に重要な貢献をしている。そのためユーザーは、パスワードを不正に閲覧されないよう保護する必要がある。

パスワードは特に保護しなければならない。

ユーザーはパスワードを入力する前に、入力中のパスワードを監視できないことを確認する必要がある。周囲にいる人に対して、距離を置くように配慮を求めること。また権限のない者に対して、もしくは委任のためにパスワードを渡してはならない。ユーザー以外の者がパスワードを知っている根拠がある場合には、ユーザーはただちにパスワードを変更しなければならない。

パスワードが不正に利用されたことが分かる根拠がある場合には、ユーザーは担当窓口に**通報**しなければならない。

ユーザーアカウントのパスワードは業務用と私用とで異なるものにすること（参照標準：*アクセス制御*）。

同僚が長期間不在にする場合であっても（病欠、休暇など）、代理の者にパスワードを渡してはならない。

4.2.5 モバイルデータキャリア

モバイルデータキャリア（例：スマートフォン、タブレット、ノートパソコン、USB メモリー、メモリーカードなど）を**放置してはならない**。それが難しい場合は、安全かつ他人の目の届かない所に保管すること。モバイルデータキャリアの**紛失**または盗難は、ただちに担当窓口に**通報**しなければならない。

モバイルデータキャリアの紛失はただちに報告すること。

ソースが信頼できない場合またはその内容や要素に不安を抱く根拠がある場合には、ユーザーはソフトウェアのダウンロードや実行、あるいは添付ファイルの展開を行ってはならない（参照標準 *通信セキュリティ*および*運用セキュリティ*）。

4.2.6 アドバイスとサポート

従業員の情報セキュリティに関する質問は、管轄の BISO に問い合わせることができる。管轄の BISO 一覧は、社員ポータルの GIS で確認できる（ポータルコード @BISO）。

質問には BISO が対応する。

5 国別規則

経営陣は各自の責任範囲として、国内法と本規程の内容が一致していることを保証しなければならない。そのために必要なプロセスを定めること。

データマネージメント、データコンプライアンスおよび情報セキュリティのテーマ分野に関連する国内法について、万一に備えて継続的な監視および監査を行うことは、国内の本社直轄のグループ会社の経営陣が単独で責任を負う。

国内法および Mercedes-Benz Group による任意の約束が、本規程に対して例外要件もしくはより厳しい要件を求める場合は、前者が優先される。規程に定められた規則が実行不可能で例外を必要とする場合、本社直轄のグループ会社の経営陣はその旨を書面にて説明し、前もって担当の組織と意見調整を行わなければならない。管轄については*ロールハンドブック*に記載されている（*第 1.6 章*）。