セキュリティ・ポリシー

技術的及び組織的セキュリティ対策
Axessは、自らが委託した外部のコンピューターセンターとの契約において、データ保護に関する特別要件を考慮することをそれぞれ約束する。内部及び外部双方のデータセンターが日本及びオーストリアに所在しているため、Axessは、GDPRに従い提供されたデータをデータ処理システム上で処理するための注文の実行に必要なあらゆる委託先の対策を講じ、データ保護に関する要件が充足されるように社内組織を構築するよう常に努力する。

セキュリティゾーン及び権限者のグループ又はアクセス認可を有する者が定められ、アクセス経路が適切に保護され、記録媒体が、安全性が保証された方法で管理及び保管されるよう確保されている。

現在、特に以下に記載する必要な対策が取られている。

1. **アドミッションコントロール**
無権限者に対し、データが処理又は利用されるシステムへのアドミッションを許可することが禁止されている。コンピュータールームは、耐震と分類されるオフィスビルに位置している。アドミッションコントロール（IT、ファシリティ及び管理者の従業員に限定）は、以下に記載する対策のいずれかにより保証される。
> 認可/チップカード

セキュリティゾーンへの立ち入りは記録される。無権限者及び社外の者（サービス技術者、コンサルタント、清掃員等）は、権限者が付き添う場合に限り、コンピュータールームに立ち入ることができる。アドミッションコントロールは、以下に記載する追加の組織的/技術的対策を利用して行われる。
> アラームシステム
> ビル監視
> 映像技術

2. **システムアクセス制御**
無権限者によるデータ処理システムの使用は、以下の方法により回避される。
> パスワード

各権限者は、自らのみが知るパスワードを有するものとし、当該パスワードを定期的に変更しなければならない。データ処理及び通信システムに係るすべての行為について自動プロトコル（ログファイル）が作成される。無権限者によるデータ転送のための装置を利用したデータ処理システムの使用は、以下の方法により回避される。
> VPN（仮想プライベートネットワーク）

3. **データアクセス制御**
データ処理システムの利用を認められた者は、アクセス認可の対象である自らのデータに独占的にアクセスでき、処理、利用及び保存中にデータを許可なく読み込み、複製、変更又は削除することができないことが保証されている。アクセス権限を有する者は、自らのアクセス権の対象となっているデータのみにアクセスすることができ、かかる制限は、以下に記載の対策により保証される。
> アクセス認可の自動検査（システム内）

4. **利用目的管理**
異なる目的において収集されたデータを、以下に記載する方法により別々に処理することが保証されている。
> ソフトウェアベース（例：顧客別）
> アクセス規制による分離（データベース原則）
> テストデータと現行データの分離
> テストシステムと現行システムの分離（技術、プログラム）

5. **仮名化**
それぞれのデータ処理について可能な限りにおいて、個人データの主要な識別機能は、各データアプリケーションにおいて取り除かれ、個別に保管される。

6. **転送制御**
記録媒体上において個人データが電子的に転送、移送又は保存されている間は、認可なく読み込み、複製、変更又は削除できないことが保証されており、また、データ転送装置によって個人データが転送されることが想定される地点でこれを確認及び検証できることが保証されている。記録媒体の発送は、登録及び添付書類により記録及び管理される。個人の記録媒体をコンピュータールームに持ち込み、使用することは認められない。記録媒体は、以下に記載する方法で破棄される。
> 磁気記録媒体の上書き及び物理的破壊（外部のサービス提供者）

インターネットが個人データの転送に利用される限りにおいて、以下のセキュリティ対策が用いられる。
> ファイアウォール
> 仮想プライベートネットワーク（VPN）

7. **入力制御**
個人データがデータ処理システムに入力、変更又は削除されたか否か、及び当該入力、変更又は削除を行った者を後日確認及び検証可能であることが保証されている。Axessは、当該目的において入力を記録する。

8. **アベイラビリティ管理**
以下に記載する対策により、個人データを不慮の破壊又は喪失から保護することが保証されている。
> 日/週/月/年次のデータバックアップ
> ストレージエリアネットワーク（SAN）
> ディスクミラーリング（特にRAID）
> 無停電電源装置（UPS）
> 過電圧フィルター
> 非常用発電設備
> 防災機器

9. **データ保護管理**
データ保護管理が設けられ、実施されていることが保証されている。データ保護管理は、以下の要素に分けられる。
> 処理活動のリスト
> 契約データ処理
> データ保護影響評価
> 事故対応管理
> データ保護違反に係る報告
> 研修
> PDCA（計画、実行、評価、改善）：定期点検

10. **事故対応管理**
責任者が想定されるシナリオに対してどのように対応するかに関して対策が取られている。これには、データのセキュリティ侵害、DoS（サービス妨害）、DDoS（分散型サービス妨害）、ファイアウォールにおけるギャップ、ウイルス又はマルウェアによる感染及び内部者による脅威が含まれる。
事故対応管理は、6つの重要な段階に分けられる。
> 準備：Axessの全従業員が、想定される事故が起こり、その際取るべき手順について研修を受け、又は知らされていること。
> 特定：事由が実際にデータ保護に関する事案であるか判断。
> 抑制：更なる被害を回避するために、当該事案によって生じる被害を抑制し、侵されたシステムを分離すること。
> 除去：原因又は事案の引き金となったものを究明し、有効な環境から侵されたシステムを取り除くこと。
> 復旧：更なる脅威が存在しないことが確認された後、侵されたシステムを有効な環境に再び統合すること。
> 習得した知識：事案報告書の作成及びチーム又は会社が当該事案から得られる教訓の分析。これにより、特定の状況下での今後の対応を改善することができる。

11. **プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト**
適切な技術的及び組織的対策が取られていることが保証されており、これにより、対応する事前設定により、原則として、個別に決定された処理目的において処理が必要な個人データのみが処理されることを確保する。
> 個人データは、契約の処理（定期入場券等）に必要な場合にのみ収集される。
> オンラインショップにおけるcookieの設定は、ユーザーの同意を得た場合にのみ可能である。
> マーケティング目的での個人データの利用は、ユーザーの能動的な同意によってのみ許可される。

12. **注文管理**
注文により処理される個人データについて、顧客の指示に従った場合に限り処理されることが保証されている。以下に記載の各種契約データ処理に関し、契約が存在する。
> 第三者によるデータ処理
> 第三者による記録媒体の破棄/処分
> 第三者による保守及び遠隔保守
> 第三者による管理/遠隔管理

注文による個人データの処理（顧客の指示に従った場合に限る。）は、以下に記載する方法により保証されている。
> 書面による指示
> オファー及び注文請書
> 仮名化

13. **再委託データ取扱者**
> CN Group CZ s.r.o.
> Agentur LOOP New Media GmbH
> DI Scheidl Alexander