GDPR有事対応支援サービス

個人データ漏洩発生! 専門家が対応をガイド

GDPR33条の遵守

GDPR33条で、個人データが漏洩したとき、または大規模なサービス停止などでデータが侵害されたときは、管理者がそれを認識した時点から72時間以内に監督機関に報告をする義務があります。更に、影響を受けたデータ主体への通知が必要なこともあります。

この初動を間違えると、その企業にとってのレピュテーションリスクだけでなく、業務停止命令、制裁金の請求、更にはデータ主体への補償と、経営に大きな影響を与えるリスクになりかねません。

特に、監督機関への報告は、できるだけ速やかに誠実に行う必要があります。インシデントへの対応は、日本だけの対応ではなく、欧州の監督機関への報告とデータ主体への通知も行う必要があるため、既存のインシデント対応の枠組みだけでは対応しきれないことも考えられます。

サービスの特長

IIJ GDPR有事対応支援サービスでは、お客様の有事対応チームへの心強いアドバイザーとして、監督機関への報告やデータ主体への通知の仕方を適切にアドバイスいたします。更に、ご要望に応じて、報告文書作成などに必要な作業をいたします。

費用

- 初期費用：4,000,000円～
- 月額費用：62,000円
- 有事対応費用：時間課金

※有事対応費用は、保険でまかなうことが可能です。詳しくは、担当営業にお問い合わせください。

個人データ侵害時の業務フローの全体像（例）

貴社の初動対応
- 個人データ、侵害の検知
- 第一報用ヒアリング・シートの作成
- IIJ緊急対応窓口に連絡（24時間365日、日英対応可能）
- IIJ作成の各種テンプレート※1利用による事実確認・自己評価

↓ エスカレーション

対応方針の決定
- 信憑性確認
- 侵害データの量と質の把握
- 調査チームの組成
- 優先すべき調査範囲・方法の決定

↓ 指示

初期調査
- 状況・影響範囲・原因の把握
- 個人へのリスク評価
- 影響緩和策の策定
- フォロー調査の検討

↓ 報告

データ侵害の認知
- データ侵害の妥当な可能性を検討
- 監督機関への報告、データ主体への通知要否の検討
- 影響緩和策の実施

↓ エスカレーション

通知要否の決定
- 通知内容・方法の確認
- 通知不要時の対応策の確認
- 説明責任のため対応経緯を文書化

↓ 段階的な通知または一括して通知※2

監督機関への通知
- 今後の対応策の相談
- データ主体に通知する際は要相談
- 他の監督機関への通知要否の検討

↓ フォロー業務に続く

不当な遅滞なき対応方針の決定と初期調査の実施（第三者からの通報前に要実施、対応遅れへの説明責任あり）

72時間以内に監督機関に報告（第三者による通報前に要通知）

（事態が深刻な場合）報告

※1：各種テンプレート
1. GDPR対応要否検討用の参考例一覧
2. GDPR対応要否チェックリスト（簡易版）
3. 情報セキュリティインシデント対応の全体像
4. 個人データ侵害検知時のフローチャート
5. 初期調査項目一覧
6. 被害拡大防止・封じ込め措置の暫定チェックリストなど

※2：個人データ侵害通知報告書（第一報）
- 侵害内容（例：データ主体・データの種類と概数）
- 侵害の影響
- 管理者が実施した影響緩和策
- データ保護責任者（DPO）の氏名と連絡先

詳しくは、以下のWebサイトをご覧ください。
https://www.iij.ad.jp/biz/gdpr-incident/

お問い合わせは、IIJインフォメーションセンターまで

IIJ
Internet Initiative Japan

TEL：03-5205-4466 受付時間：9:30～17:30（土・日・祝日・年末年始を除く）
E-Mail：info@iij.ad.jp
URL：www.iij.ad.jp
株式会社インターネットイニシアティブ

※本内容は予告なく変更することがあります。（2019年1月作成）
※表示価格には、消費税は含まれておりません。
※記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。

IIJ-CAT031-0002