

5分でわかる 個人情報保護法とGDPR





近年、セキュリティリスクの高まりを受け、多くの企業でセキュリティ対策への意識が高まっています。セキュリティ事故にはさまざまなものがありますが、中でも企業の業績に大きな影響を与えてしまう可能性が高いものが、個人情報の漏洩です。個人情報の漏洩が発生してしまった場合、多額の損害賠償が発生するだけでなく、企業の信頼が損なわれ、存続が危うくなってしまいうケースすらあります。

このような事態を防ぐために定められた法律が「個人情報の保護に関する法律」（個人情報保護法）です。このような法律やガイドラインは各国で定められており、EUではGDPR（General Data Protection Regulation：一般データ保護規則）というものが定められています。

こうした流れの中、個人情報を安全に運用するための環境構築は急務と言えるでしょう。業務への影響を最小限に抑えつつ、対策を講じていかななくてはなりません。そこで本資料では、個人情報保護法の概要や対応策、そこで役立つCRMの機能を紹介します。

個人情報保護法とGDPR(一般データ保護規則)の概要

まず、個人情報関連の法律について解説します。2019年時点で企業が把握しておくべきルールは、「改正個人情報保護法」および「GDPR(一般データ保護規則)」の2つといえます。以下は、それぞれの概要と比較表です。

改正個人情報保護法の概要

日本国内において、個人情報の利用目的や利用範囲、管理、第三者への提供などをルールとして定めた法律です。改正前(2017年5月29日)までは、取り扱っている個人情報の件数が5,000件以上という条件があったため、一部の大手企業のみが対象となっていました。しかし、改正後は件数の条件が撤廃され、中小企業も含めたすべての組織が対象になっています。

GDPR(一般データ保護規則)の概要

一言で説明すると、「個人データの処理と移転に関するルール」といえます。2つの柱(EU地域以外への個人データ移転に対する厳しい制限、情報主体の権利強化)が特徴で、巨額の制裁金(最大で企業の年間売上高の4%または2000万ユーロのうちいずれか高い方)が課されることも見逃せません。

改正個人情報保護法とGDPRの比較

	改正個人情報保護法	GDPR(一般データ保護規則)
適用対象組織	<ul style="list-style-type: none"> 日本国内において、個人情報を扱うすべての組織(国、地方公共団体、独立行政法人等および地方独立行政法人や、民間事業者) 	<ul style="list-style-type: none"> EU居住者からデータを収集する組織 データ管理者の代理としてデータを処理する組織 データ主体(個人) <p>※EU居住者の個人データを収集、もしくは処理する場合はEU域外の拠点を置く組織にも適用される</p>
適用対象データ	<p>日本国内に居住する個人の個人情報</p> <p>※但し 国外犯処罰規定あり</p>	<p>EU在住者の個人データに関する取扱い</p> <p>※EU域外じでの対応について厳しい罰則あり(罰則を参照)</p>

	改正個人情報保護法	GDPR (一般データ保護規則)
個人データの定義	<ul style="list-style-type: none"> ・生存する個人に関する情報及び、個人識別符号が含まれるもの ・生存する個人に関する情報： 氏名、生年月日、住所、電話番号、ファックス番号、所属団体や氏名から本人特定に繋がるメールアドレス、防犯カメラの画像や音声データ、クレジットカード情報、銀行口座番号など ・個人識別符号： 顔認証データ、指紋認証データ、運転免許証番号、基礎年金番号、マイナンバー、旅券番号、保険証、パスポート番号など 	<ul style="list-style-type: none"> ・氏名、識別番号、所在地データ、メールアドレス、オンライン識別子 (IPアドレス、クッキー)、クレジットカード情報、パスポート情報 ・身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因など ※Cookieやビデオ映像など無記名の個人データも該当
個人データの取得、利用、管理に関するルール	<ul style="list-style-type: none"> ・利用目的を具体的に特定し、通知・公表する。 ・特定した利用目的の範囲内でのみ利用可能。 ・取得済みの個人情報を他の目的で利用する場合には、本人の同意が必要。 ・要配慮個人情報の取得には、本人の同意が必要。 <p>※要配慮個人情報＝人種、信条、社会的身分、病歴、前科、犯罪被害情報のほか、不当な差別や偏見が生じないように特に配慮を要するもの</p>	<ul style="list-style-type: none"> ・個人データの処理および保管に当たり、適切な安全管理措置を講じなければならない。 ・目的の達成に必要な期間を超えて、個人データを保持し続けてはならない。 ・定期的かつ大量の個人データを取扱う組織などでは、データ保護オフィサーを任命する必要あり。
個人データの移転に関するルール	<ul style="list-style-type: none"> ・本人以外の第三者に渡すときは、原則として本人の同意が必要 ・国外の第三者への提供には本人の同意や個人情報保護委員会規則に則った方法などが必要 	<ul style="list-style-type: none"> ・越境データ移転 (EEA域外への個人データ移転) は原則として違法 ・上記移転にはSCC (標準契約条項) やBCR (拘束的企業準則) の締結、明確な本人同意などが必要

	改正個人情報保護法	GDPR (一般データ保護規則)
個人データ 侵害発生時の対応	<ul style="list-style-type: none"> 個人情報保護委員会への速やかな報告 本人への速やかな報告 	<ul style="list-style-type: none"> 72時間以内に監督機関へ通知 データ主体への通知
代理人規定	<ul style="list-style-type: none"> 対応規定なし 	<ul style="list-style-type: none"> EU域内に拠点を持たない者が、EU域内の個人データを取り扱う場合には、EU域内に代理人の設定が必要
罰則	<ul style="list-style-type: none"> 国からの命令に違反した場合 6ヶ月以下の懲役又は30万円以下の罰金 虚偽の報告等をした場合 30万円以下の罰金 不正な利益を図る目的で個人情報データベース等を提供、又は、盗用した場合 1年以下の懲役又は50万円以下の罰金 	<ul style="list-style-type: none"> 企業の年間売上高の4%、もしくは200万ユーロ (約23億円) のいずれか高い方を制裁金として支払う

出展:

https://blogs.manageengine.jp/gdpr_diy_001/
https://www.ppc.go.jp/files/pdf/28_setsumeikai_siryou.pdf

日本企業に求められる個人情報保護法への対応とは？

日本国内において企業が特に意識すべきなのは、改正個人情報保護法といえます。改正個人情報保護法への対応では、主に以下のような点に注力していくべきでしょう。



基本方針の策定

個人情報保護法に則り、組織としての基本方針を策定する。



個人データ取り扱いに関する規律の整備

既存の業務プロセス、マニュアルなどを見直し、個人データの取得や利用、保存にかかる基本的な方法を整備する。



組織的安全管理処置

組織体制の整備や個人データの運用、漏洩時の体制、チェック方法などを整備する。



人的安全管理処置

従業員への教育や就業規則の改定などを通じ、個人データの取り扱いに関する留意事項について周知徹底を行う。



物理的安全管理処置

個人データの保管場所や保管方法、持ち運び時の規定を整備する。

この中でも、「個人データ取り扱いに関する規律の整備」については、多くの施策が必要になるでしょう。特に、データの取得、利用、移転などに関して必要となる「本人の同意」を厳格に適用するためには、業務プロセスやシステムの変更が必要です。また、これらに関する手間をいかに抑えるかが、個人情報保護法への対応させるためのポイントといえます。

個人情報保護法とGDPRに対応可能なZoho CRMの機能

Zoho CRMでは、個人情報保護法とGDPRに則したさまざまな機能を標準搭載しており、業務負担を最小限に抑えた対応が可能です。

Webフォーム

Webフォーム作成機能により「個人情報を求める理由」をあらかじめ明記できます。

また、ダブルオプトインを有効にしたメール送信機能で、受信者がリンクをクリックすることで個人データの収集およびサービス提供に同意したことを検知できます。

フォームの詳細

フォーム名*

フォーム設置先のURL* ?

遷移先ページのURL* ?

担当者の割り当て* ユーザーの選択 見込み客の割り当てルールを作成する

[割り当てルールを作成する](#)

通知

担当者への通知

[メールテンプレートを作成する](#)

プライバシーの同意

「データのプライバシー」から適法根拠を設定し、顧客がデータのプライバシーに同意したかどうかをステータスで管理することができます。

GDPRコンプライアンス 有効

組織のコンプライアンス設定では、顧客の個人情報の処理・管理する方法を策定するのに便利な機能です。

概要 環境設定 同意フォーム

データ処理の基本設定 (合計同意獲得数: 500) 見込み客 ▾

適用不可 (38) 100

表示

適用可 (147) 同意: 100 その他: 300

表示 表示

すべての確認状況: 100

保留中

35/
100

確認待ち

40/
100

確認済み

25/
100

個人情報のカテゴリー別管理

個人情報をカテゴリー別に管理することができます。個人情報保護法における「要配慮情報」などのように、特に取り扱いに注意が必要な個人情報は、カテゴリーを分けることで適切に管理することができます。

標準
一行
保存して閉じる 保存

作成 クイックリンク

見込み客情報

姓

メール

識別番号

作成者

住所情報

会社名

郵便番号

項目ラベル *

名

入力文字数の制限 *

255 最大225文字

必須

値の重複を禁止する ○

個人情報の識別

一般個人情報 重要個人情報

項目の暗号化 ?

ヒントの表示

詳細設定 ▾

プレビュー

完了
キャンセル

同意確認メールの自動送信

顧客に対し、データ取得の同意を求めるメール作成・送信を半自動的にを行い、同意に対するステータス状況も確認することができます。

プレビュー ×

ZYLKER

ご登録いただき誠にありがとうございます。
製品に関するご案内、ebook、Webinerなどイベントのご案内などをお送りいたします。
ご希望の連絡方法を下記より選択ください。

メール
 電話
 アンケート

ご希望などございましたらこちらに入力してください。

個人データの取り扱いについて同意の上、「送信」をクリックしてください。

本稿では、個人情報保護法とGDPRの概要や、企業に求められる対応について紹介してきました。個人情報の不適切な取り扱いは、ビジネス上の大きなリスクとなるでしょう。情報漏洩が発生してしまった場合、多額の罰金が科されるだけでなく、企業の信用力も低下させてしまうからです。そのため、事前にしっかりと対応しておくことが大切です。セキュリティ対策がしっかりされているZoho CRMを活用し、業務プロセス・システム面の整備を効率的に進めてみてはいかがでしょうか。




15日間無料でお試しいただけます。

[登録はこちら](#)

自社での活用方法に関するご質問や製品デモのご要望などがございましたら、
ゾーホージャパン株式会社営業窓口までお気軽にお問い合わせください。

ゾーホージャパン株式会社 営業窓口

 0120-007-542

 sales@zoho.jp

Zoho、Zoho CRM のロゴマークは Zoho Corporation Pvt. Ltd. の登録商標または商標です。記載されている商品名、各製品名は各社の登録商標または商標です。また、当社製品には他社の著作物が含まれていることがあります。

本冊子の内容は、2025年5月8日現在のものです。本書に記載された仕様、デザイン、その他の内容については、改良のため予告なしに変更される場合があります。