

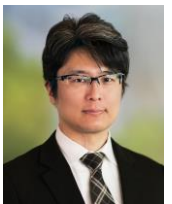
Client Alert

20 December 2018

本クライアントアラートに
関するお問い合わせ先



高瀬 健作
パートナー
03 6271 9752
kensaku.takase@bakermckenzie.com



達野 大輔
パートナー
03 6271 9479
daisuke.tatsuno@bakermckenzie.com



菅 礼子
アソシエイト
03 6271 9696
ayako.suga@bakermckenzie.com

ドイツ当局、GDPR に基づく初の罰金を命じる

ドイツ・バーデン＝ヴュルテンベルク州のデータ保護当局（DPA）がドイツで初めて EU 一般データ保護規則（GDPR）に基づいて罰金（2 万ユーロ）を命じました。インターネットのチャットサービスを提供する事業者である "knuddels.de" がユーザーのパスワードを暗号化せずに保存していたことに対する罰金です。

同社は 2018 年 7 月にハッキングに遭い、同年 9 月には盗まれた約 33 万人のユーザーのメールアドレスやパスワードなどの個人情報がハッカーによって公開されました。同社は、GDPR 第 33 条及び第 34 条に基づき直ちに DPA とユーザーに通知しましたが、DPA に情報を開示する過程で、同社がユーザーのパスワードを暗号化していなかったことが判明し、GDPR 第 32(1)(a)条に違反すると判断されました。

当該違反には、GDPR 第 83(4)(a)条により、1000 万ユーロ以下又は前会計年度の全世界年間売上上の 2%以下の罰金が科されます。DPA は、罰金を決定するにあたり、同社が DPA に対して全面的に透明性を確保し協力したこと、同社が法的な要件と DPA の勧告の両方を実施し、直ちに個人情報の保護レベルを上げたこと、セキュリティ違反による同社に対する財務的な影響（罰金を含む）は全体で 10 万ユーロ単位であったこと、同社が追加的な措置について DPA にさらに協力する意思があること、などを考慮したとしています。DPA は、罰金は実効的で抑止的効果があるものでなければならないが、他方で事案の程度に応じたものでなければならない、と強調しています。

なお、ドイツ連邦個人情報保護法第 43(4)条は、GDPR 第 33 条及び第 34 条に基づく通知は、データ管理者（data controller）の同意がない限りデータ管理者（data controller）に罰金を科す行政手続において利用されてはならない、と規定しています。この規定が本件でどのように考慮されたのか、DPA の発表からは明らかではありません。本件を前提とすれば、実務において企業がドイツ連邦個人情報保護法第 43(4)条による保護を享受できる場面は極めて少ないことになってしまうでしょう。

GDPR などの厳しい規制に 対応するためのコンプライ アンス・eラーニングプロ グラムのご案内

ベーカーマッケンジーでは、グローバル規模のコンプライアンス・トレーニング・プログラムの構築・導入支援を通じて、世界を舞台に事業を展開する企業が、一般データ保護規則（GDPR）対応など、主要なコンプライアンス規制に対する意識を高め、各国の従業員の行動に変化を起こすためのサポートを行っています。当ファームの専門家の監修のもと、各企業の目的に沿ったコンプライアンス・トレーニング・プログラムを設計いたします。詳細は[こちら](#)よりご確認ください。本件に関するご相談またはトライアルご希望の際は、[こちら](#)までご連絡ください。

© 2018 Baker McKenzie. ベーカー・マッケンジー法律事務所（外国法共同事業）はスイス法上の組織体であるベーカー・マッケンジー インターナショナルのメンバーファームです。ベーカー・マッケンジー法律事務所（外国法共同事業）及びベーカー・マッケンジー インターナショナルのその他のメンバーファームは、日本においては弁護士法人ベーカー・マッケンジー法律事務所を通じて業務を提供します。専門的知識に基づくサービスを提供する組織体において共通して使用されている用語例に従い、「パートナー」とは、法律事務所におけるパートナーである者またはこれと同等の者を指します。同じく、「オフィス」とは、かかるいずれかの法律事務所のオフィスを指します。

本資料に含まれている情報及びデータは一般的な情報であり、当事務所の法的アドバイスや意見を提供するものではありません。法律及び税務に関わる参考情報や対策については本資料のみに依拠すべきでなく、本資料の受信者は必要に応じ別途弁護士のアドバイスを受けなければなりません。