個人データ取扱要領　（例）

平成●年●月●日

第１章　総則

（目的）

第１条　本要領は、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）及び個人情報の保護に関する法律についてのガイドライン（以下「個情法ガイドライン」という。）に定める個人データの安全管理措置について、必要な措置を定めるものとする。

（定義）

第２条　用語の定義は、個人情報保護法及び個情法ガイドラインに定めるところによる。

※必要に応じて、マイナンバーに関する法令等を追記したりする。

第２章　管理体制

（責任者の設置）　※個情法ガイドライン安全管理措置 8-3(1)に対応

第３条　個人データの取扱いに関する責任者（以下「責任者」という。）を置くこととし、●●をもって充てる。

２　責任者は、個人データの管理に関する事務を総括するとともに、自ら本要領に定められた事項を遵守し、かつ従業者に遵守させるために、本要領に定める措置その他必要な措置を実施する責任を負う。

（社内報告体制の整備）　※個情法ガイドライン安全管理措置 8-3(4)に対応

第４条　別紙１により、次に掲げる組織体制を整備する。

⑴　従業者が、個人情報保護法、個人情報の保護に関する法律施行令（平成 15 年政令第 507 号。以下「政令」という。）、個人情報保護委員会が定める規則（以下「規則」という。）、個情法ガイドライン及び本要領に違反している事実又は兆候を把握した場合の責任者への報告連絡体制

⑵　個人データの漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための報告連絡体制

２　従業者は、個人情報保護法、政令、規則、個情法ガイドライン及び本要領に違反している事実又は兆候を把握した場合及び個人データの漏えい等の事案の発生又は兆候を把握した場合、別紙１により明確にした報告連絡体制に従って報告する。

第３章　従業者の教育　※個情法ガイドライン安全管理措置 8-4 に対応

第５条　責任者は、個人データの取扱いに関する留意事項について、従業者に周知するとともに適切な教育を行う。

※秘密保持に関する事項を就業規則等に盛り込むことも考えられます。

第４章　個人データの取扱い

（本要領に従った運用及び取扱状況の確認）※個情法ガイドライン安全管理措置 8-3(2)、(3)に対応

第６条　責任者は、本要領に従って個人データが取り扱われていることを確認する。

※個人情報データベース等を情報システムで取り扱う場合、個人データの取扱いの検証を可能とするために、情報システムの利用状況（ログイン実績、アクセスログ等）を記録することを自社の状況に応じて盛り込むことが大切です。

（個人データを取り扱う区域の管理）　※個情法ガイドライン安全管理措置 8-5(1)に対応

第７条　個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置を講ずる。

（機器及び電子媒体等の取扱い）　※個情法ガイドライン安全管理措置 8-5 (2)、(3)に対応

第８条　個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するため、施錠可能な場所への保管等の措置を講ずる。

２　個人データが記録された電子媒体又は書類等を持ち運ぶ場合、パスワードによる保護、封緘等により、容易に個人データが漏えいしないよう安全な方策を講じる。

（廃棄等）　※個情法ガイドライン安全管理措置 8-5(4)に対応

第９条　責任者は、個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合には、確実に廃棄されたことを確認する。

（委託先の監督）　※個情法ガイドライン 3-3-4 に対応

第 10 条　個人データの取扱いの全部又は一部を委託する場合には、委託先を選定する際に、委託先が個人情報保護法に基づき●●自らが果たすべき安全管理措置と同等の措置が講じられることについて、あらかじめ確認する。

２　個人データの取扱いの全部又は一部を委託する場合には、委託先に安全管理措置を遵守させるための必要な契約を締結する。

３　個人データの取扱いの全部又は一部を委託した場合、委託先における個人データの取扱状況を把握する。

４　前各項に定める委託先が当該委託業務を再委託する場合（再委託先が更に再委託する場合も含み、以下本条において同じとする。）は、委託先を通じて再委託先についても適切に監督する。

※第４項を遵守するために、委託先が再委託をする場合は、事前に報告を受けること又は承認を行うこと及び委託先が再委託先の個人情報取扱状況を適切に監督すること等を委託契約に盛り込むことが考えられる。

※再委託先が不適切な取扱いを行った際は、委託元による法違反と判断され可能性がある。

（アクセス制御等）　※個情法ガイドライン安全管理措置 8-6(1)、(2)、(3)、(4)に対応

第 11 条　従業者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行う。

２　個人データを取り扱う情報システムを使用する従業者が、正当なアクセス権を有する

者であることを、ユーザーＩＤ、パスワード等により認証する。

３　個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入したうえで、自動更新機能等を活用し、ソフトウェアを最新状態に保つことなどにより、情報システムを外部からの不正アクセス等から保護する。

４　メール等により個人データの含まれるファイルを送信する場合には当該ファイルへのパスワードを設定するなど、情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用する。

（安全管理措置の見直し）　※個情法ガイドライン安全管理措置 8-3(5)

第 12 条　責任者は、個人データの取扱状況について、定期的に点検する。

２　前項の点検の結果を踏まえ、安全管理措置の見直し及び改善に取り組む。

※安全管理措置の見直しに際しては、中小企業のための自己点検チェックリストを再度活用し、自社の状況を確認することも有効です。

第５章　各管理段階における措置　※個情法ガイドライン安全管理措置 8-2 に対応

第 13 条　別紙２の様式により個人データを取り扱う事務の流れを整理し、管理段階ごとに、取扱方法、責任者・担当者及びその任務等について、安全管理措置を織り込んだ事務マニュアルを定める。

※各部署における事務ごとに、具体的な取扱方法・留意点を定める。
※複数の事務をまとめて作成することも考えられる。

附則

本要領は、平成●年●月●日から施行する。