

「プロジェクト個人情報取扱基準」作成マニュアル

個人情報に係る業務を行う場合、プロジェクト個人情報責任者は「個人情報管理規則」、および本マニュアルに従い「プロジェクト個人情報取扱基準」を作成して下さい。
本マニュアルに定義のない用語に関しては、「個人情報管理規則」等の定義に従うものとします。

1. 作成単位

- ・基本的に「帳票・ファイル名」ごとに「プロジェクト個人情報取扱基準」を作成します。
- ・個人情報の取得～利用・提供～廃棄・返却に至る全プロセス内の個人情報に係る全ての「帳票・ファイル名」を対象にしてください。
- ・ただし、個人情報の取扱いが同じ場合、複数の帳票・ファイルを一つの「プロジェクト個人情報取扱基準」にまとめることができます。
- ・個人情報を取扱わないプロジェクトについては、「プロジェクト個人情報取扱基準」を作成する必要はありません。

2. 新規、変更の区分

- ・新規プロジェクトで「プロジェクト個人情報取扱基準」を新規作成の場合は「新規」のを、既存プロジェクトの「プロジェクト個人情報取扱基準」を変更する場合は、「変更」のを にします。
- ・変更の場合は、既存の「プロジェクト個人情報取扱基準」の No をかっこ内に記載します。

3. プロジェクトの概要

「プロジェクトの期間」: プロジェクトの終了時期が明確でない場合は、開始時期のみ記載します。Ex. 2004/8/1～

プロジェクト個人情報総責任者: 委託(注)される場合、発注側の責任者

注: 委託とは個人情報を含む業務を外注委託することを言います。

プロジェクト個人情報責任者: 弊社のプロジェクト責任者

4. 個人情報の特定と取扱い

帳票・ファイル名等(内容)

- ・原則として紙の場合は帳票名を、デジタルの場合はファイル名を記載します。
- ・帳票名・ファイル名を特定できない場合は、内容を記載します。
Ex. 銀行殿の顧客の普通預金口座取引明細

媒体/形式

- ・紙、MO、CD-R、FD、オンラインなど。

取扱件数

- ・取扱う個人情報を以下の区分に応じ分類し、該当する区分に○をします。
- ・各分類ごとに取り扱い件数を記載します。件数は、現在保有している数ではなく、数年先を見越して扱う数値を概数で表示します。

一般的な個人情報	氏名、性別、住所、出生地(県名)、生年月日、家族構成(続柄)、親族関係、電話番号、会社名、職業、地位、社員番号、ID番号、写真(顔など)、声(声紋など)、指紋など
センシティブな個人情報	結婚、学歴、成績、能力、クラブ活動、昇格・降格等、賞罰、容姿、体格、性格、血液型、収入・資産状況、持家・借家の別、各種団体加入状況、趣味、交友関係、各種名簿情報(卒業者名簿、会員名簿等)、口座番号、クレジットカード番号、保険証番号など
特定の機微な個人情報	思想、信条、宗教、人種、民族、門地、本籍地(都道府県に関する情報を除く)、身体・精神障害、犯罪歴、離婚、労働組合への加盟、労働争議への参加、集団示威行為への参加、請願権の行使、政治的権利の行使、保健医療、性生活など

個人情報内容

- ・ 氏名、住所、電話番号、生年月日、性別は、該当項目の を にします。
- ・ その他の個人情報を取扱う場合は、できるだけ詳細に () 内に記載します。

作成者

- ・ の帳票・ファイル名等の作成者。

管理責任者

- ・ の帳票・ファイル名等の管理責任者。通常はプロジェクト個人情報責任者に同じ。

アクセス権限範囲

- ・ の帳票・ファイル名等へのアクセス可能者名。

保管方法

- ・ の帳票・ファイル名等への保管方法（保管場所）。
Ex. ファイル、 サーバ、 倉庫など

保管期間

- ・ の帳票・ファイル名等の保管期間。委託の場合は弊社処理範囲内での保管期間。

廃棄・返却

- ・ の帳票・ファイル名等の廃棄・返却方法を記載します。廃棄、返却の記録を残す場合は、記録帳票名を記載します。

個人情報の取得目的

- ・ 個人情報の取得は、取得目的を明確に定め、その目的達成に必要な限度において行わなければならないため、利用目的を明確に特定する。
Ex. 総合テスト、運用テストを実施するため

個人情報の通知、同意の取得方法

- ・ 個人情報を取得した場合は、本人に対し、一定の内容の事項を通知し、同意を得なければなりません

委託された場合：直接取得でないので『委託業務のため該当せず』の を にします。

直接取得の場合：以下の事項の通知、同意取得の方法を記載します。

- a) 当社内個人情報に関する管理者又はその代理人の氏名・職名・所属・連絡先。
- b) 取得目的。
- c) 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約有無。
(当社は、個人情報の提供は行わない)
- d) 個人情報の委託を行うことが予定される場合には、その旨を記載。
- e) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果。
- f) 個人情報の開示を求める権利及び開示の結果、情報が誤っている場合に訂正又は削除を要求する権利の存在並びに当該権利を行使するための具体的な方法

取得手段

- ・ 不正な手段により取得してはならないため、契約などの取得方法（どういう手段で）、収集先（誰から）を記述します。
- ・ 委託の場合は、個人情報の授受の記録の有無を記載する。記録がある場合は、記録の名称、方法を記載します。
Ex. 「個人情報受払簿」に預かる個人情報の内容を記載し、顧客のサインを頂く。
- ・ 随時に入手する場合は、上記取得方法で『～で随時に入手する』を記入し、委託でまとめて入手する場合は、『入手した時点で、「 」に記録する』と記入します。
- ・ インターネットを使用して個人情報を入手するときは『安全対策上SSLを使用する』と記入します。
- ・ インターネットを使用して個人情報を入手或いは利用する際にクッキー（Cookie）を使用

する場合は、『クッキーを使用する』と記入すると共に、当該WebページのURLを記載。また、『P3Pを使用してプライバシーポリシーを明示すること』と記入します。
注) SSL : Secure Socket Layer、P3P : Platform for Privacy Preferences

正確性の確保手段

- ・ 個人情報は正確かつ最新の内容に保つ必要があるため、情報のアップデート頻度、取得方法などを記述する。委託された場合は、顧客から要求されている規程類、開発業務規則又は運用業務規則、安全対策で正確性を確保します。

Ex. (顧客が要求する管理文書名) 開発業務規則、安全対策で正確性を確保

安全性の確保手段

- ・ 入退管理、アクセス者の限定、ID・パスワードの設定、定期的なアクセスログの取得、他部署との送受信には暗号をかける、施錠保管、管理台帳の設置などの帳票・ファイルの安全対策を具体的に記載します。
- ・ 安全性に関して顧客より要求されている規程類がある場合は、これを引用します。

Ex. 開発環境での 銀行殿の顧客の個人情報の取り扱いは禁止、本番環境での総合テスト、運用テストは、顧客立会いのもと実施

従業者・委託先の管理、監督

- ・ 個人情報の安全管理が図られるよう、従事者及び委託先に対する必要かつ適切な管理、監督手段について記述します。

従業員に対する周知徹底手段

教育の実施など周知徹底する内容を記述します。

委託先(もしあれば)管理方法

委託する個人情報の内容、委託方法に応じ委託先の管理方法を記載します。

Ex. 別途チェックリストを作成し提出を求める。

当社従業員と同様の教育を実施する。

定期的に個人情報の取扱いについて監査を実施する。

当社と委託先との個人情報の授受について記録を残す。

個人情報の開示、訂正、利用停止等の手続きの作成と本人への通知方法

委託された場合：直接取得でないので『委託業務のため該当せず』のを にします。

直接取得の場合：開示、訂正、利用停止等の手続き及び訂正又は削除を行った場合の本人への通知方法を記載します。

開示については、本人確認の方法を明確にする。

特記事項

- ・ 顧客固有の管理規程など上記のほか特に留意すべき点があれば記載します。

顧客固有の管理規定等

- ・ ~ を記載する際に顧客固有の管理規定等を参照した場合は、当該規定等の名称を記載します。

5. その他

- ・ 上記記載事項の文書量が多くなる場合は、別途手順書を作成してプロジェクト個人情報取扱基準から引用します。
- ・ 入退管理などサイト毎に決定する必要がある場合は、各サイト毎に記載してください。

附則

1. この規則は、平成 17 年 12 月 15 日から施行する。
2. 平成 18 年 11 月 1 日に改定、施行する。
3. この規則を改廃する場合には、従業員の意見を聴いて行う。

以 上