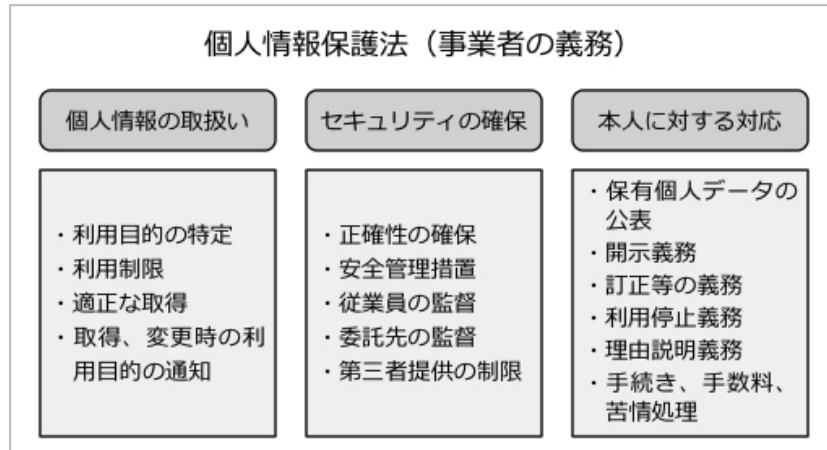


1 事業者の義務と取り組み

【事業者の義務と取り組み】（概要）



1）事業者の義務

- ・ 短期保有個人データの除外条件が廃止されたため、**全事業者が対象**
- ・ **差別や悪用**につながる方法の利用禁止（不正利用対策）
- ・ 漏えい時に個人情報保護委員会への**報告**および本人への**通知**
- ・ **第三者提供**を行う場合の規制への対応
- ・ 公開項目として**事業者の住所、代表者名**等の追記

2）個人（本人）の権利確保

- ・ 開示方法として**電磁的記録**を追加、**第三者提供記録**の追加対応
- ・ **利用停止**等要件追加への対応

3）個人情報の利活用促進

- ・ 「**仮名加工情報**」追加で、柔軟な内部利用を推進
- ・ 「**個人関連情報**」が定義され、その利活用法について検討

4）ペナルティの強化

- ・ **罰則の強化と罰金の引き上げ**

5）その他

- ・ **海外提供の場合**には本人の同意と情報提供が必要
- ・ 個人情報の**海外移転**について検討

2 対策のポイント1 個人情報取扱事業者とは（適用範囲の拡大）

【法の適用範囲の拡大で、全ての事業者が対象】

従来個人情報取扱事業者から除外された『データベース内の個人情報で識別される個人の数が過去6ヵ月間のいずれの日でも5,000を超えない事業者』という除外規定が撤廃されたため、個人情報の取扱いの件数を問わず、**全ての事業者が個人情報保護法の対象**となりました。

これによって、従来対応が義務付けられていなかった中小事業者や個人情報の取扱数が少ない事業者を含めた**全ての事業者が対象**となりました。

事業者の対応として、個人情報保護委員会は事業者に求められる対策（中小以外の事業者向け）と中小事業者向けの対策案を**ガイドラインの（別添）講ずべき安全管理措置として公開**しています。（対策点検チェックリスト参照）

私たちは、個人情報を取り扱うリスクを正しく認識し、法と組織の目的に沿って利用方法と安全管理について意思決定し、有効な対策を実施しなければなりません。

【個人情報保護方針（プライバシーポリシー）の策定の必要性】

策定は義務化はされていませんが、**個人情報保護方針（プライバシーポリシー）**を策定することで、組織のあるべき姿、保護の目的と方針を明らかにし、組織の状況に応じた安全管理活動、顧客の信頼性獲得につなげていくことが大切です。

ポリシー策定のために

- ・従業員の個人情報も、個人情報保護法に準じた取扱いが求められます。
- ・事業者によって具体的な対応は異なりますが、まず以下のような作業が必要です。

守るべきもの（個人情報）の特定

- ・どのような個人情報を扱っているか、保持しているかを棚卸しする

個人情報保護法の理解

- ・法令で示された諸対応について理解する

脅威の特定と影響の評価

- ・保持している個人情報にどのようなリスクがあるか評価する

利用プロセスに沿って安全管理措置を決定

- ・利用目的の整理・特定と伝達手段の選定などを含めたルールを整備

必要事項を公開し、マネジメントしていく

- ・ポリシー（方針）を策定し、安全管理措置の策定・実施、公表（HP等）

【関連資料の例】

- ・プライバシーポリシー（個人情報保護方針）

3 対策のポイント2 第三者提供時の確認および記録の作成義務

過去の大型漏えい事件等で、名簿業者等が介在し違法な個人データの取引が行われていたことが明らかになったことで、トレーサビリティを確保するために、事業者は個人データの第三者提供の確認及び記録の作成が義務付けられました。

【記録作成と確認】

取引先や顧客から取得した個人データの第三者提供を行う場合

あらかじめ第三者提供を行うことに対して本人の同意を得ることが必要です。

記録としては、以下が必要です。

- ①提供した年月日
- ②提供先の氏名、住所
- ③提供情報の氏名等本人を特定できる事項
- ④提供個人データの項目等

・第三者提供を行う際には、提供側・受領する側双方において記録を作成し保存します。

事業者が第三者から個人データの提供を受ける場合

違法に入手された個人データの流通を抑止するため、第三者（提供元）がその個人データを取得した経緯等を確認し、記録を作成しなければなりません。

記録としては、以下が必要です。

- ①提供受けた年月日
- ②提供元の氏名、住所
- ③データ取得の経緯
- ④提供情報の氏名等本人を特定できる事項
- ⑤提供個人データの項目
- ⑥個人情報保護委員会により公表されている事実等

・提供する立場だけでなく、受領する立場の場合も注意する必要があります。

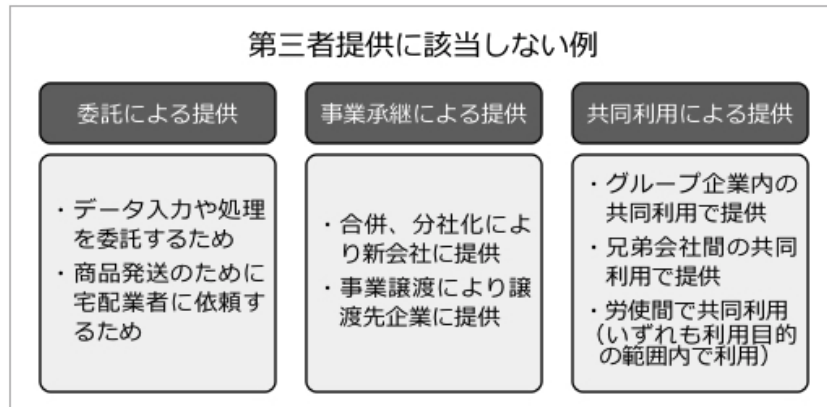
既存の契約書などで記録事項を充たしている場合は、それが記録として認められます。また事業者は、必ずしも、台帳のようなものを用意する必要はありませんが、保存義務を履行するための方法（請求への対応）を、明確にして実施する必要があります。

【記録義務が適用されない例外】

従業員の口座に給与を振り込みや送付等の公的なサービス利用の場合は、提供者が最終的に本人に提供することを意図した上で、受領者を介在して提供を行っているものなので、記録義務は適用されません。

これらの詳細情報については、個人情報保護委員会の見解が、FAQやQ&Aによって提供されていますので、都度参照・確認しましょう。

また、業務でどのような場合が第三者提供、委託、共同利用等に当たるのかを明確にしておきましょう。



● 個人情報保護法の第三者提供と委託の考え方

【第三者提供とは】

「第三者提供」とは、自社が保有する個人情報を第三者に渡し、受け取った第三者は、その個人情報を（利用目的の範囲内で）自由に使える状態にある場合を指します。

（留意点）

- ・ **第三者提供を行う際は**、個人情報の取得元（本人）に対して、「**第三者提供を行うこと**」について、**同意を得ておく必要**があります。（取得時には第三者提供を予定していなかったが、取得後に第三者提供を行うことになった場合は、第三者提供を行うことに同意を取り直し、同意が得られた個人の個人情報のみ、第三者提供が可能）
- ・ **第三者提供を受けた側も**、個人情報の取得時に同意を得た**利用目的の範囲内でのみ**、取り扱うことができます。

【委託とは】

ビジネスでは、顧客を頂点として数多くの事業者がサプライチェーンを構成しています。その中では、業務委託（BPO）と言われるサービスも多様化しており、個人情報を扱う際の各々の責任範囲の明確化が必要になります。

前提として、業務が委託や受託なのかを明確にし、そのプロセスのリスクを認識することが必要です。また、そのリスク対策を行うためには、**誰が責任を負うのか、行うのか、コストを負担するのか**等を事業者間で合意しておかなければ、トラブルが起こった場合に迅速な対処ができないため注意が必要です。

「**委託**」は、自社の業務の一部を第三者に代行してもらうために、自社保有する個人情報を提供する場合（委託元の利用目的でのみ利用する）を指し、本人の同意は不要です。

（留意点）

- ・ 第三者提供ではないため、提供側と受領側に対する「**記録義務**」は発生しません。
- ・ **委託元（個人情報の提供側）は、委託先（個人情報を受領し、業務の一部を代行する側）の「監督責任」が生じます。**

具体的には・・・

- ・ **対応能力の事前確認、評価**
委託先が個人情報保護法を遵守しており、適切に個人情報を取り扱う能力があるかどうか「安全管理措置の実施」の確認と評価が必要です。
- ・ **契約締結**
委託元と委託先の間で、しっかりと**委託契約を締結し、責任分界点の設定や業務終了後のデータの破棄等**についても取り決めを行います。

- ・ **監督責任**

第三者提供のような記録義務は生じませんが、**委託先の監督**のためには積極的に自らが記録をつける等の対応は必須となります。

【委託に該当しないケース】

- ・ 委託先が委託提供された個人データを委託元の区別なく混ぜて取り扱う場合は**第三者提供**になります。
- ・ 委託先で本人ごとに他のデータと突合することや、委託先が自らの目的で委託された個人データを加工すること、匿名加工情報等を作成することはできません。

【関連資料の例】

- ・ 個人情報取扱規定

4 対策のポイント3 オプトアウトによる第三者提供の制限強化

オプトアウトで入手した個人データを第三者提供する場合には、**個人情報保護委員会への届出を行い、公表されない限り行えなくなりました。**

過去の大量情報漏えい事件で、名簿業者の介在による不正な個人データの取引が行われていた事実が明らかになったことが契機となり、オプトアウトについての改正が行われました。

名簿業者等から個人情報を購入する際には十分な注意が必要です。個人情報保護委員会
で公表されている事業者からの購入が求められますが、いずれにしてもその目的や社内
での管理プロセスを十分に検討しなければなりません。

【オプトアウトの制限】

オプトアウトによる第三者提供の制限	
第三者提供の禁止	①要配慮個人情報 ②不正取得された個人データ ③オプトアウトにより提供された個人データ
届け出・通知	①個人情報保護委員会への届け出、公表 ②本人への通知 （事業者の住所、代表者名、データの取得方法） ③本人が容易に知り得る状態（HPでの公表）
事項の変更	①個人情報保護委員会への届け出、公表 ②改めて本人に通知または公表
同意の取得	オプトアウト要件があれば不要
提供の停止	本人からの要請があれば停止しなければならない

【オプトアウトする場合の個人情報保護委員会への届け出】

届出の方法

- ・届出書および当該届出書に記載するべき事項を記録したCD-Rの両方を提出
- ・届出書様式および記入要領は個人情報保護委員会HPに掲載
- ・届出書は個人情報保護委員会HPからダウンロードした届出書様式のみ受け付け

届出の内容（提供および提供をやめた場合も、委員会に届け出る）

- ・個人情報取扱事業者の氏名または名称、住所、法人の代表者名
- ・第三者提供すること
- ・個人データの項目
- ・第三者に提供される個人データの更新の方法
- ・提供を開始する予定日

5 対策のポイント4 要配慮個人情報の取得制限

【要配慮個人情報とは】

要配慮個人情報とは、人種、信条、社会的身分、病歴、犯罪の経歴、犯罪によって害を被った事実、その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報と定義されています。

EUデータ保護指令では、機微情報（センシティブ情報）の取得が原則禁止され、日本がEUから「十分性の認定」を得るためには、これを法律上定める必要があり、改正されました。

しかし、これらの情報は様々なシーンで取得されてしまうケースがあり、気づかないでSNS等で公開してしまうこともあるので注意が必要です。

組織内でも、**健康診断情報、障害情報や採用時の履歴情報**等、慎重な取り扱いが必要なものを特定し、適切に安全管理しましょう。

- ・ 本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実
- ・ 不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述 等

要配慮個人情報

【該当するもの】

- ・ 人種
- ・ 信条
- ・ 社会的身分
- ・ 病歴
- ・ 犯罪の経歴
- ・ 犯罪により害を被った事実
- ・ 身体障害、知的障害、精神障害（発達障害を含む）その他の個人情報保護委員会規則で定める心身の機能の障害があること
- ・ 医師により行われた疾病の予防および早期発見のための健康診断その他の検査の結果
- ・ 健康診断等の結果に基づき、または疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導または診療もしくは調剤が行われたこと

- ・ 本人を被疑者または被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと
- ・ 本人を少年法に規定する少年またはその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと
- ・ 遺伝子検査結果等のゲノム情報

【該当しないもの】

- ・ 本籍地
- ・ 国籍
- ・ 反社会的勢力に該当する事実
- ・ 運転免許証の条件等・臓器提供意思の確認欄
- ・ 労働組合への加盟・性生活
- ・ 介護に関する情報

【要配慮個人情報の取扱い】

差別等の要因となる要配慮個人情報の取得は**同意のもとに取得**しなければなりません。

また、オプトアウト手続きによる**第三者提供は禁止**されています。

【ポイント】

- ・ 要配慮個人情報とは、個人情報のうち、**差別や偏見につながる可能性を持つ情報**のこと。
- ・ 他の個人情報と同じく、**利用目的が明確**で、その情報を取得しなければ事業ができない、当初の目的を達成できない、という場合は取得する必要があるが、「この情報は

取得しておいたほうが良いかもしれない」レベルでの取得はすべきではありません。

- ・取得をしてはならないのではなく、取得・取扱いの際には、明確な同意のもとで取得し、取扱いには、より一層の注意が必要です。

【例外事項】

ただし、法令に基づく場合や、以下の同意の取得が困難な場合の同意は不要です。

- ・人の生命、身体または財産の保護のために必要
- ・公衆衛生の向上、児童健全育成推進のために必要
- ・国の機関、地方自治体またはその委託を受けた者が事務を遂行する必要
- ・本人、国の機関、地方自治体、個人情報保護委員会規則で定める者によって公開されている場合

【関連資料の例】

- ・個人情報取扱規定
- ・要配慮個人情報管理基準一覧表