# 個人情報保護指針

はじめに

平成 27 年 9 月に個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成 27 年 9 月 9 日法律第 65 号）が成立し、個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）（以下、旧法という。）の全面施行から 12 年振りに改正（平成 27 年 9 月 9 日法律第 65 号）がされ、平成 28 年 1 月 1 日に、その一部（第 5 章 個人情報保護委員会）が施行、平成 29 年 5 月 30 日に全面的に施行された。

今後、対象事業者は、個人情報保護委員会の指導、監督の下で個人情報を適切に取扱い、その取扱いに関する本人からの苦情に関しては、当事者として自ら対応しなければならない。

しかし、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならないという法の定めに対して、場合によっては当事者同士で解決が図れない事や本人と一定の距離を置いた対応が必要となる事も生じることであろう。

そこで、公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会（以下「ＮＡＣＳ」という。）は認定個人情報保護団体としての認定を受け、客観的な苦情処理を担う組織となることで、本人と対象事業者双方にとって有益となるよう機能を果たしていくことを決議した。

個人情報保護法第 53 条では、認定個人情報保護団体に対して、対象事業者の個人情報等の適正な取扱いの確保のために、個人情報に係る利用目的の特定、安全管理のための措置、開示等の請求等に応じる手続その他の事項又は匿名加工情報に係る作成の方法、その情報の安全管理のための措置その他の事項に関し、消費者の意見を代表する者その他の関係者の意見を聴いて、この法律の規定の趣旨に沿った指針（以下「本指針」という。）を作成し公表することが求められている。

そこで、当協会としては「本指針」を定めた。また、個人情報保護法第 53 条では認定個人情報保護団体に対して、対象事業者に個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとらなければならないとされていることから、当協会においては、対象事業者が本指針を遵守しなければならないことを「Ⅲ　対象事業者の義務」として規定した。

**認定個人情報保護団体としての業務**

当協会は、認定個人情報保護団体の業務として、個人情報保護法第 47 条に規定されている下記の事項を行う。

業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）の

1.個人情報の取扱いに関する個人情報保護法第 52 条の規定による苦情の処理

2.個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供

3.そのほか、対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

**認定個人情報保護団体として扱う苦情**

1.個人情報の本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときには、下記の事項に関する処理を行う。

a.相談に応じること

b.申出人に必要な助言をすること

c.その苦情に係る事情を調査すること

d.当該対象事業者に対し、苦情の内容を通知してその迅速な解決を求めること

2.苦情の解決について必要があると認めるときには、下記の事項に関する処理 を行う。

a.当該対象事業者に対し、文書若しくは口頭による説明を求めること

b.当該対象事業者に対し、資料の提出を求めること

（対象事業者は、個人情報保護法第 52 条第 3 項に基づき当協会からの求めについて、正当な理由がなく拒むことはできないものとする。）

**対象事業者になる（当協会の傘下に入る）ことの意味**

**対象事業者の利点**

- 当協会が第三者機関として関与することで迅速・円滑な苦情の解決が期待できる。
- 当協会から適切な情報が提供されることによって、適切な個人情報保護の取組が維持できる。

**個人情報の本人の利点**

- 当協会が第三者機関として関与することで迅速・円滑な苦情の解決が期待できる。
- 安心して個人情報の開示ができる環境整備が期待できる。

## Ⅰ　本指針の趣旨、目的、基本的考え方

### １．本指針の趣旨

本指針は、「個人情報の保護に関する法律」（平成１５年法律第５７号。以下「法」という。）を踏まえ、「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成２８年個人情報保護委員会告示第６号。以下「通則ガイドライン」という。）を基礎とし、法第５３条１項の規定に基づき、対象事業者が行う個人情報の適正な取扱いの確保に関する活動を支援するための具体的な留意点・事例等を示すものである。

なお、本指針は対象事業者における実例に照らした内容であるため、本指針に記載のない事項及び関係条文については「通則ガイドライン」、「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（平成２８年個人情報保護委員会告示第７号）、「同ガイドライン（第三者提供時の確認・記録義務編）」（平成２８年個人情報保護委員会告示第８号）及び「同ガイドライン（匿名加工情報編）」（平成２８年個人情報保護委員会告示第９号）をそれぞれ参照されたい。（以上の４本のガイドラインおよび「個人データの漏えい等の事案が発生した場合等の対応について」（平成29年個人情報保護委員会告示第１号）を合わせて、以下「ガイドライン等」という。）

### ２．本指針の構成及び基本的考え方

個人情報の取扱いについては、法第３条において、「個人情報が、個人の人格尊重の理念の下に慎重に取り扱われるべきものである」とされていることを踏まえ、個人情報を取り扱うすべての者は、その目的や様態を問わず、個人情報の性格と重要性を十分認識し、その適正な取扱いを図らなければならない。

本指針では、法の趣旨を踏まえ対象事業者における個人情報の適正な取扱いが確保されるよう、遵守すべき事項及び遵守することが望ましい事項をできる限り具体的に示しており、対象事業者においては、法令、「個人情報の保護に関する基本方針」（平成１６年４月２日閣議決定。以下「基本方針」という。）及び本指針の趣旨を踏まえ、個人情報の適正な取扱いに取り組む必要がある。

具体的には、対象事業者は本指針の中で、「しなければならない」、「必要がある」等と記載された事項については、厳格に遵守することが求められる。また、【その他の事項】については、達成できるよう努めることが求められる。

### ３．本指針の対象となる事業者の範囲

本指針が対象としている事業者（以下「対象事業者」という。）は、ＮＡＣＳを認定個人情報保護団体として、その傘下となることを希望した者としている。

また、当該対象事業者が個人情報の取扱いの委託を行う場合は、業務の委託に当たり、本指針の趣旨を理解し、本指針に沿った対応を行う事業者を委託先として選定するとともに委託先事業者における個人情報の取扱いについて定期的に確認を行い、適切な運用が行われていることを確認する等の措置を講ずる必要がある。

### ４．本指針の対象となる「個人情報」の範囲

本指針では、「特定の個人を識別することができる」の解釈においては、直接的もしくは間接的に、とりわけ氏名、識別番号、位置データ、オンライン識別子といった識別子を参照することによって、または身体的、生理的、遺伝的、精神的、経済的、文化的ならびに社会的なアイデンティティに特有の１つまたは複数の要素を参照することによって、特定の個人を識別することができることをいい、位置データやオンライン識別子も「個人情報」として、対象事業者が事業の用に供するすべてのものを対象とする。
また、法令上「個人情報」とは、生存する個人に関する情報であり、対象事業者の義務等の対象となるのは、生存する個人に関する情報に限定されている。しかし、本人が死亡した後においても、対象事業者が本人の情報を保存している場合には、漏えい、滅失又はき損等の防止のため、個人情報と同等の安全管理措置を講ずるものとする。

５．認定個人情報保護団体としての権限行使との関係

①対象事業者の指針運用状況の把握

ＮＡＣＳは、対象事業者による本指針の遵守状況確認のため、以下について報告を求めることができるものとする。

□個人情報を適正に管理するための社内規程の策定状況
□個人情報保護管理責任者（CPO または DPO）の設置状況
□安全管理体制の状況
□個人情報に関する苦情・相談窓口の設置状況
□個人情報の適正管理についての従業者教育の実施状況
□その他本指針の遵守状況に確認の為に必要な事項

②漏洩等事故が発生した場合の対応

対象事業者において、個人情報の漏えい等の事案が発生した場合は原則として、ＮＡＣＳに対し、当該事実の発生を知ってから３営業日以内に通知を行わなければならない。

③個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供

ＮＡＣＳは、個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供を行う。対象事業者は、この情報提供を受けて、従業者への研修を１年に１回以上行う必要がある。

④対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

ＮＡＣＳは、対象事業者に対して、必要に応じて本指針の遵守状況について調査等を実施することができるものとする。

本指針中、対象事業者の義務とされている内容を個人情報取扱事業者としての義務を負う対象事業者が遵守しない場合、個人情報保護委員会から、法第４０条から第４２条の規定に基づき、「報告徴収」、「立入検査」、「指導・助言」、「勧告」及び「命令」を行われることがある。

これに対して、ＮＡＣＳでは以下のとおり本指針を遵守してもらうための指導、勧告その他の措置を行なう。

- ＮＡＣＳは、本人その他の関係者から対象事業者の個人情報等の取扱いに関する苦情について申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めるものとする。
- ＮＡＣＳは、前項の申出に係る苦情の解決について必要があると認めるときは、当該対象事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることができるものとする。
- 対象事業者は、NACS から前項の規定による求めがあったときは、正当な理由がないのにこれを拒んではならない。

６．対象事業者が行う措置の透明性の確保と対外的明確化

法第３条では、個人の人格尊重の理念の下に個人情報を慎重に扱うべきことが指摘されている。

対象事業者は、個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等）を策定し、それらを対外的に公表することが求められる。また、個人情報の取扱いに関する明確かつ適正な規則を策定し、本人から当該本人の個人情報がどのように取り扱われているか等について知りたいという求めがあった場合は、当該規則に基づき、迅速に情報提供を行う等必要な措置を行うものとする。

個人情報保護に関する考え方や方針に関する宣言の内容としては、対象事業者が個人の人格尊重の理念の下に個人情報を取り扱うこと及び関係法令及び本指針等を遵守すること等、個人情報の取扱いに関する規則においては、個人情報に係る安全管理措置の概要、本人等からの開示等の手続、第三者提供の取扱い、苦情への対応等について具体的に定めることが考えられる。

なお、利用目的等を広く公表することについては、以下のような趣旨があることに留意すべきである。

① 対象事業者が本人の個人情報を利用する意義について本人等の理解を得ること。

② 対象事業者において、法を遵守し、個人情報保護のため積極的に取り組んでいる姿勢を対外的に明らかにすること。

７．責任体制の明確化と窓口の設置等

対象事業者は、個人情報の適正な取扱いを推進し、漏えい等の問題に対処する体制を整備する必要がある。このため、個人情報の取扱いに関し、専門性と指導性を有し、対象事業者の全体を統括する組織体制・責任体制を構築し、規則の策定や安全管理措置の計画立案等を効果的に実施できる体制を構築するものとする。

また、本人に対しては、個人情報を取得する時、利用を開始する時に個人情報の利用目的を説明するなど、必要に応じて分かりやすい説明を行う必要があるが、加えて、本人が疑問に感じた内容を、いつでも、気軽に問い合わせできる窓口機能等を確保することが重要である。また、個人情報の取扱いに関す

る相談は、対象事業者が提供するサービスの内容とも関連している場合が多いことから、個人情報の取扱いに関し本人からの相談や苦情への対応等を行う窓口機能等を整備するとともに、その窓口がサービスの提供に関する相談機能とも有機的に連携した対応が行える体制とするなど、本人の立場に立った対応を行う必要がある。

この場合、対象事業者の苦情相談窓口と合わせて、認定個人情報保護団体となるＮＡＣＳについて以下の通り掲載するものとする。

【記載例】
当社の認定個人情報保護団体は、下記の通りです。
公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会
連絡先：03-6434-1125

なお、個人情報の利用目的の説明や窓口機能等の整備、開示の求めを受け付ける方法を定める場合等に当たっては、障害のある方にも配慮する必要がある。

ＮＡＣＳに苦情解決の申し出があったときは、当該苦情の対象となる対象事業者に通知し、苦情内容について必要な調査を依頼し、その結果の報告を求めると同時に、解決案の提示を求める。(苦情申立人が対象事業者及び関係者への通知を希望しない場合は、この限りではない。)。

ＮＡＣＳは、対象事業者が提出した調査結果及び解決案の内容が不十分であると認めるときは、不十分な点を明示して、再度調査のうえ結果の報告を求める。

対象事業者は、正当な理由がある場合を除き、苦情処理の為の協力要請に応じなければならないものとする。

８．遺族への死者の個人情報の提供の取扱い

法は、ＯＥＣＤ８原則の趣旨を踏まえ、生存する個人の情報を適用対象とし、個人情報の目的外利用や第三者提供に当たっては本人の同意を得ることを原則としており、死者の情報は原則として個人情報とならないことから、法及び本指針の対象とはならない。しかし、本人が死亡した際に、遺族から個人情報が含まれる諸記録について照会が行われた場合、対象事業者は、本人の生前の意思、名誉等を十分に尊重しつつ、特段の配慮が求められる。このため、本人が死亡した際の遺族に対する個人情報の提供については、社会通念に照らした上で遺族に対して諸記録の提供を行うものとする。

９．個人情報が研究に活用される場合の取扱い

近年の科学技術の高度化に伴い、研究において個人情報を利用する場合が増加している。

法第７６条第１項においては、憲法上の基本的人権である「学問の自由」の保障への配慮から、大学その他の学術研究を目的とする機関等が、学術研究の用に供する目的をその全部又は一部として個人情報を取り扱う場合については、法による義務等の規定は適用しないこととされている。従って、この場合には本指針もまた適用されるものではないが、これらの場合においても、法第７６条第３項により、当該機関等は、自主的に個人情報の適正な取扱いを確保するための措置を講ずることが求められており、これに当たっては、各研究分野等の関連指針とともに本指針の内容についても留意することが期待され

る。

１０．遺伝情報に触れる場合の取扱い

遺伝情報については、本人の遺伝子・染色体の変化に基づく体質、疾病の発症等に関する情報が含まれるほか、その血縁者に関わる情報でもあり、その情報は生涯変化しないものであることから、これが漏えいした場合には、本人及び血縁者が被る被害及び苦痛は大きなものとなるおそれがある。したがって、遺伝学的検査等により得られた遺伝情報の取扱いについては、UNESCO 国際宣言等、各研究分野等の関連指針及び関係団体等が定める指針を参考とし、特に留意する必要がある。

１１．他の法令等との関係

対象事業者は、個人情報の取扱いにあたり、法、基本方針、ガイドライン等及び本指針に示す項目のほか、個人情報保護又は守秘義務に関する他の法令等（刑法、関係資格法、介護保険法等）の規定を遵守しなければならない。

また、事業の管理者の監督義務や業務委託に係る契約債務等を遵守しなければならない。

１２．他の認定個人情報保護団体との関係

法第４７条においては、個人情報取扱事業者等の個人情報等の適正な取扱いの確保を目的とする業務を行う法人等は個人情報保護委員会の認定を受けて認定個人情報保護団体となることができることとされている。また、認定個人情報保護団体となる団体等は、傘下の事業者を対象に、個人情報保護に係る普及・啓発を推進するほか、法の趣旨に沿った指針等の自主的なルールとして定めたり、個人情報の取扱いに関する相談窓口を開設するなど、積極的な取組を行うことが期待されている。

これに対して、ＮＡＣＳでは傘下の対象事業者に対して本指針の遵守を要求するが、傘下となる対象事業者がＮＡＣＳ以外の団体等の傘下となることを妨げない。

１３．保有する個人情報に対する所有権の移譲

事業者の破産等により、当該事業者の所有権が債権者に移る場合に、当該事業者が保有する個人情報がその対象となることは、個人情報の本人が望まない場合があり得る。そのため、NACS の傘下の対象事業者は以下の措置をとらなければならない。

① 対象事業者が個人情報の取扱いを委託する際には、委託先に対して当該個人情報は抵当権を設定できない旨を契約において締結すること。
② 対象事業者に対して債権を持つ者に対して、対象事業者が保有する個人情報は抵当権を設定できない旨を契約において締結すること。
③ 対象事業者は、破産等により財産の所有権を失う場合に備えて、対象事業者が保有する個人情報は当該事案の発生時にＮＡＣＳに対して無償で提供する旨を契約において締結すること。

## Ⅱ　用語の定義等

本指針における用語の定義およびその解説は、「Ⅲ　対象事業者の義務等」において示すものを除き、法およびガイドライン等によるものとする。

Ⅲ 対象事業者の義務等

「個人情報の保護に関する法律」（平成１５年法律第５７号。以下「法」という。）を踏まえ、以下のガイドライン（ガイドライン等）を順守すること。

- 「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成２８年個人情報保護委員会告示第６号。）
- 「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（平成２８年個人情報保護委員会告示第７号）
- 「個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）」（平成２８年個人情報保護委員会告示第８号）
- 「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」（平成２８年個人情報保護委員会告示第９号）
- 「個人データの漏えい等の事案が発生した場合等の対応について」（平成29年個人情報保護委員会告示第１号）

さらに、下記の要件を上乗せして適用すること。

**1． データ主体の権利強化**

**ア 「個人情報」および「個人データ」の概念の拡張**

「個人データ」の概念を拡張させて、データベース等を構成するものであることを要件とせず、単一の個人に関する情報でも「個人データ」に該当するものとしてガイドライン等を読み替えて適用しなければならない。

また、「特定の個人を識別することができる」の解釈においては、直接的もしくは間接的に、とりわけ氏名、識別番号、位置データ、オンライン識別子といった識別子を参照することによって、または身体的、生理的、遺伝的、精神的、経済的、文化的ならびに社会的なアイデンティティに特有の１つまたは複数の要素を参照することによって、特定の個人を識別することができることをいい、位置データやオンライン識別子も「個人情報」としてガイドライン等を適用しなければならない。

**イ 削除権（忘れられる権利）**

取得時の利用目的に照らして個人情報の保有の必要性がなくなった場合や、データ主体が同意を撤回した場合等に、データ主体が管理者に対し、自己に関する個人情報の消去を請求し、当該個人情報の拡散を防止するための措置を請求する権利を認めなければならない。

**ウ データポータビリティの権利**

データ主体が、①自らが提供した個人情報について、管理者から一般的に利用され、機械的に可読である体系的なデータ形式（ex. CSV形式等）にて提供を受ける権利と、②ある管理者（移行元のサービス事業者のプラットフォーム）から妨害されることなく、他の管理者（移行先の新規のサービス事業者のプラットフォーム）に対して、自らの個人情報を直接移行させる権利を認めなければならない。

**エ　取扱いに対する異議申立権**

データ主体は、ダイレクトマーケティングの目的で自己の個人情報が取り扱われ、またはそのような目的で「プロファイリング」に利用されている場合、管理者に対し、異議を申し立てることができることを認めなければならない。

なお、「プロファイリング」とは、自然人に関する特定の個人的傾向を評価するために（特に、当該自然人の職務上の成果、経済状況、健康状態、個人的嗜好、関心、信頼性、行動、位置情報もしくは活動に関する傾向を分析または予測するために）、個人情報を利用して行うすべての個人情報の自動処理をいう。

**オ　プロファイリングに基づく措置に服さない権利**

「プロファイリング」等の自動化された取扱いに基づく決定が、自らに法的効果または重大な影響を与える措置となる場合には、データ主体が、これに服しない権利を認めなければならない。

なお、「プロファイリングに基づく措置」とは、スマートフォンアプリ等を利用したオンラインサービスの普及に伴い、アルゴリズムやAIを用いて、オンラインサービス、スマートフォンやIoT（Internet of Things）機器から収集され蓄積された個人に関するデータをプロファイリングすることで、自動的に個人を類型化して管理し、その結果、単なるターゲットマーケティング目的での利用に止まらず、与信評価に基づく融資の決定、健康状態の評価に基づく保険契約における保険加入の可否および保険料率の決定、行動モニタリングに基づく人事評価の決定等の、個人にとって重大な影響を受ける決定事項が、機械的かつ自動的に行われることをいう。

**2.　個人情報の取扱いの厳格化**

**ア　本人の同意**

管理者は、個人情報をデータ主体から直接書面で取得する場合に限らず、取扱う個人情報に関しては、データ主体が、その利用目的に同意しているようにしなければならない。

また、16歳未満の子どもについては、保護者の同意を得なければならない。

**イ　個人情報の取り扱いに関する義務等**

管理者は、データ主体の権利の保護を確実にする取扱方法で、適切な技術的かつ組織的な措置を実施することを十分に保証する取扱者のみを個人情報の取り扱いの委託先として利用するようにしなければならない。

また、取扱者への委託に際して契約を締結し、特に取扱者が以下の事項を行うように規定しなければならない。

① 法令によって取扱いの実施が要求されていない限り、第三国または国際機関への個人情報の移転に関することを含め、管理者からの書面による指示においてのみ個人情報を取り扱うこと。当該法律によって取扱いの実施が要求される場合、取扱者は、当該法律が重要な公共の利益に基づき

通知を禁止していない限り、事前に当該法的要件を管理者に通知しなければならないこと。

② 個人情報を取り扱うことを許可された者が機密保持を確約するか、または適切かつ法定の機密保持義務の下で管理されることを保証すること。

③ 管理者として要求されているのと同等のすべての対策をとること。

④ 他の取扱者を従事させることに関して以下の条件を遵守すること。

- 取扱者は、事前の特定又は管理者の一般的な書面の許可なしに他の取扱者を従事させてはならない。一般的な書面の許可の場合、取扱者は、他の取扱者の追加又は代替に関するあらゆる意図された変更について管理者に通知しなければならず、それによって管理者に当該変更に不服を申し立てる機会を提供するものとする。
- 取扱者が管理者の代わりに行う特定の取扱い活動を他の取扱者に従事させるならば、契約又は管理者と取扱者間のその他法的行為で規定されているのと同じデータ保護義務が、契約に基づくその他法律行為によって他の取扱者に課されていなければならない。特に、取扱いが本規則の要件と合致するような適切な技術的及び組織的対策の実施を十分に保証するように規定していること。

⑤ 取扱いの性質を考慮し、可能な限りにおいて、管理者が第3 章に定められたデータ主体の権利行使の要求に応じる義務を履行するため、適切な技術的かつ組織的な措置によって管理者を支援すること。

⑥ 取扱いの性質および取扱者の利用可能な情報を考慮し、義務（取扱いの保護、個人情報侵害の監督機関への通知、データ主体への個人情報侵害の通知、データ保護影響評価、事前協議）の遵守を確実にすることにおいて管理者を支援すること。

⑦ 管理者の選択により、取扱いに関連したサービスの提供終了後にすべての個人情報を消去または管理者に返却することおよび、法令が個人情報の保存を要求しない場合に限り、存在する複製物を消去すること。

⑧ 本条項に定められた義務の遵守を証明するとともに、管理者または管理者により委任された他の監査人によって実施される調査を含めた監査への準備および寄与を行うために必要なすべての情報を管理者が入手可能にすること。

「個人情報取扱事業者」としての管理者から個人情報の取扱いの受託を受けた「委託先」となる取扱者は、事前の特定または管理者の一般的な書面の承諾なしに他の取扱者を従事させるといった再委託を禁止する必要がある。

また、他の取扱者に再委託する場合には、当該取扱者に契約で規定されているのと同じデータ保護義務が、契約によって他の取扱者に課されていなければならない。

**ウ 情報処理の記録義務**

管理者またはその代理人には、個人情報の取扱いに関し、以下の事項を書面（電磁的記録を含む。）にて記録しなければならない。ただし、従業員の数が250名未満の中小規模の企業等には適用しない。

① 管理者（その代理人、データ保護オフィサー）等の氏名・名称および連絡先

② 利用目的
③ データ主体の種類および個人情報の種類
④ 個人情報が開示されるまたは開示されうる場合の提供先の種類
⑤ 第三国または国際機関への個人データ移転の事実等
⑥ 可能であれば、データの種類ごとの消去の予定期限
⑦ 可能であれば、技術的・組織的安全管理措置の概要

また、取扱者またはその代理人には、書面にて、以下の事項の記録しなければならない。ただし、従業員の数が250名未満の中小規模の企業等には適用しない。

① 取扱者および管理者（それらの代理人、データ保護オフィサー）等の氏名・名称および連絡先
② 管理者のために実施している取扱いの種類
③ 第三国または国際機関への個人データ移転の事実等
④ 可能であれば、技術的・組織的安全管理措置の概要

**ウ 個人データの漏えいの通知義務等**

管理者は、個人データの漏えいが発生した場合には、原則として、ＮＡＣＳに対し、当該事実の発生を知ってから３営業日以内に通知を行わなければならない。具体的には、少なくとも以下のような事項を通知しなければならない。

① 個人データの漏えいの性質（可能であれば、関係するデータ主体の種類と概数、関係する個人データの種類と概数）
② データ保護オフィサーの氏名・連絡先
③ 個人データの漏えいにより想定される影響
④ 個人データの漏えいに対する対処措置（漏えいによる影響を軽減するための対策）

また、取扱者においては、自らの管理下において個人データの漏えいが生じ、当該事実の発生を知った場合には、遅滞なく管理者に通知することを義務付ける必要がある。

管理者は、個人データの漏えいに関する事実ならびにその影響および対応策を含めて、すべての個人データの漏えいについて書面で記録する義務を負い、当該書面をもって監督機関が上記の義務の遵守状況を確認できるようにしなければならない。

また、個人の権利および自由に対し、高いリスクを生じさせるおそれがある場合には、管理者は、遅滞なく影響を受けた個人に対して通知する義務もあり、その際には、少なくとも上記の②ないし④の事項について通知する必要がある。

**エ データ保護・バイ・デザイン／デフォルト**

データ保護・バイ・デザイン（Data protection by design）として、管理者は、データ主体の権利を保護するために、個人データの取扱方法の決定時点と取扱時点のいずれの時点においても、たとえば仮名化のように、適切な技術的かつ組織的な対策を実施しなければならない。（安全管理のための措置

であって「匿名加工」ではない。）
なお、そのような対策としては、たとえばデータ最小化のように、データ保護の原則を効果的な方法で履行すること、および必要な保護措置を個人データの取扱いの中に組み込むことが求められる。
また、データ保護・バイ・デフォルト（Data protection by default）として、管理者は、既定で具体的な特定の利用目的のために必要な個人データのみが取り扱われることを確実にするために、適切な技術的かつ組織的な対策を実施しなければならない。

**オ　データ保護評価の実施**

新しい技術を用いた取扱いが、自然人の権利および自由に対し、高いリスクを及ぼすおそれがあると想定される場合には、管理者は、取扱いに先立ち、予定されている取扱作業に対する個人データの保護に与える影響評価（Data protection impact assessment、以下、「DPIA」という。）を実施しなければならない。特に、プロファイリングを含めた自動処理に基づいて自然人に関する個人的側面が体系的かつ広範囲に評価され、その評価に基づいて当該自然人に法的効果または重大な影響を与える決定がなされる場合や、特別な種類の個人データ（いわゆる機微情報）または有罪判決および犯罪に関する個人データを大規模に取り扱う場合、第三者が立ち入れない場所において大規模なモニタリングを行う場合には、DPIAを実施する必要がある。

**カ　データ保護オフィサーの設置義務**

管理者または取扱者の主要事業において、①その性質、適用範囲および／または目的によって、大規模にわたるデータ主体の定期的かつ系統的なモニタリングが必要となる場合、②機微情報等の「特別な種類」の個人データまたは犯罪関連データの大規模な取扱いが必要となる場合には、データ保護オフィサー（Data Protection Officer、以下「DPO」とする。）を設置しなければならない。
なお、「特別な種類」の個人データとは、人種、民族、政治的思想、宗教的信条、労働組合の加入、遺伝データ、生体情報、健康、性生活、性的指向に関するデータをいう。
また、DPOは、専門家としての資質に基づいて指名されるものとし、特にデータ保護法および慣例に関する専門知識ならびに事業者における個人データの取扱いを、独立した立場で監督・指導する業務を遂行する能力を有する必要がある。

## Ⅳ 本指針の見直し等

### １．必要に応じた見直し

個人情報の保護に関する考え方は、社会情勢や国民の意識の変化に対応して変化していくものと考えられる。このため、法及び本指針の運用状況等も踏まえながら、本指針についても必要に応じ検討及び見直しを行うものとする。

### ２．本指針を補完する事例集の作成・公開

ＮＡＣＳは、対象事業者における個人情報の保護を推進し、対象事業者における円滑な対応が図られるよう、本指針を補完する事例集を作成し、ホームページにおいて公表する。

### ３．匿名加工情報に関する自主ルール

匿名加工の手法、データ処理等については、今後、個人情報保護委員会事務局による事務局レポート等も参考としたうえでＮＡＣＳとして自主ルールを作成するものとする。