

日本DPO協会第23 回個人情報保護セミナー
講演「データ保護責任者(DPO)を巡る
近時の動向と実務への示唆」

講師：弁護士法人北浜法律事務所
弁護士 生田 美弥子 先生(当協会顧問)
弁護士 藤原 成和 先生

2024年2月15日(木) 15:00～16:00

あいさつ「DPOの役割について」
一般社団法人日本DPO協会代表理事
堀部 政男

(一橋大学名誉教授・元個人情報保護委員会委員長)

個人情報保護基本方針とDPO①

- 「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、令和4年4月1日一部変更)を見ると、「1 個人情報の保護に関する施策の推進に関する基本的な方向」の中の「2.法の基本理念と制度の考え方」の一つである「4.④ データガバナンス体制の構築」において、DPO等に次のように言及している。
- 「上記③の自律的な取組に当たり、デジタル社会においては、ビジネスモデルや技術の革新等も著しいため、個人情報等の取扱いに関する政策や個人情報等を取り扱う事務及び事業並びにシステム構築等の際には、透明性と信頼性の確保が特に重要である。

個人情報保護基本方針とDPO②

- 各主体においては、政策、事務及び事業並びにシステム構築等の目的、個人が得ることが期待される便益やプライバシーに対するリスクを明確にし、それらをわかりやすく、丁寧に説明することが重要になる。そのためには、解決しようとする課題と、その課題を解決するために取り扱う個人情報等のデータとの関係を明確化する観点から、データの内容や性質、量や範囲の必要十分性、データの流れ、データの取扱いに関わる者の範囲、データの利用目的、安全管理レベル等の事前評価のため、PIA（個人情報保護評価又はプライバシー影響評価）の手法を用いることや、CPO（最高プライバシー責任者）やDPO（データ保護責任者）等の個人データの取扱いに関する責任者を設置することが有効であり、これらによるデータガバナンスの体制を構築することが重要である。」

個人情報保護基本方針とは

- 「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、令和4年4月1日一部変更)
- 個人情報保護法第3章 個人情報の保護に関する施策等
- 第1節 個人情報の保護に関する基本方針
- 第7条 政府は、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、**個人情報の保護に関する基本方針**(以下「基本方針」という。)を定めなければならない。
- 2 基本方針は、次に掲げる事項について定めるものとする。
 - 一 個人情報の保護に関する施策の推進に関する基本的な方向
 - 二 国が講ずべき個人情報の保護のための措置に関する事項

- 【第三号から第八号まで省略】
- 3 内閣総理大臣は、個人情報保護委員会が作成した基本方針の案について閣議の決定を求めなければならない。
- 4 内閣総理大臣は、前項の規定による閣議の決定があったときは、遅滞なく、基本方針を公表しなければならない。
- 5 前二項の規定は、基本方針の変更について準用する。
- 【2003年制定当時の個人情報保護法の第7条第3項は、「内閣総大臣は、国民生活審議会の意見を聴いて、基本方針の案を作成し、閣議の決定を求めなければならない。」となっていた。】

GDPR (PPC仮訳) のDPO

- Section 4 Data protection officer 第4 節 データ保護オフィサー
- Article 37 Designation of the data protection officer 第37 条 データ保護オフィサーの指名
 - 1. The controller and the processor shall designate a data protection officer in any case where:
 - 1. 管理者及び処理者は、以下の場合において、データ保護オフィサーを指名しなければならない:
 - (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - (a) 公的機関又は公的組織によって行われる場合。ただし、裁判所がその司法上の権限を行使する場合を除く取扱い;

- (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- (b) 管理者又は処理者の中心的業務が、その取扱いの性質、範囲及び又は目的のゆえに、データ主体の定期的かつ系統的な監視を大規模に要する取扱業務によって構成される場合;又は、
- (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
- (c) 管理者又は処理者の中心的業務が、第9条による特別な種類のデータ及び第10条で定める有罪判決及び犯罪行為と関連する個人データの大規模な取扱いによって構成される場合。

- 【第37条第2項から第7項まで省略】
- Article 38 Position of the data protection officer 【省略】
- 第38 条 データ保護オフィサーの地位
- Article 39 Tasks of the data protection officer
- 第39 条 データ保護オフィサーの職務
- 1. The data protection officer shall have at least the following tasks:
- 1. データ保護オフィサーは、少なくとも、以下の職務を行わなければならない:
 - (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (a) 管理者又は処理者及び取扱いを行う従業者に対し、本規則及びそれ以外のEU 若しくは加盟国のデータ保護条項による義務を通知し、かつ、助言すること;

- (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- (b) 取扱業務に関与する職員の責任の割当て、意識向上及び訓練、並びに、関連する監査を含め、本規則の遵守、それ以外のEU 又は加盟国の個人データ保護条項遵守、並びに、個人データ保護と関連する管理者又は処理者の保護方針の遵守を監視すること；
- (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- (c) 要請があった場合、第35 条によるデータ保護影響評価に関して助言を提供し、その遂行を監視すること；

- (d) to cooperate with the supervisory authority;
- (d) 監督機関と協力すること;
- (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
- (e) 取扱いと関連する問題に関し、監督機関の連絡先として行動すること。第36条に規定する事前協議、適切な場合、それ以外の関連事項について協議することを含む。
- 2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. 2. データ保護オフィサーは、その職務を遂行する際、取扱いの性質、範囲、過程及び目的を考慮に入れた上で、取扱業務と関係するリスクに関し、適正に注意を払う。

EDPB Guidelines on Data Protection Officers ('DPOs'), PPC 個人データの取扱いに関する責任者・責任部署の 設置に関する事例集(事例集)

- EDPB Guidelines on Data Protection Officers ('DPOs'),
- PPC データ保護オフィサーに関するガイドライン(仮訳)
- (https://www.ppc.go.jp/files/pdf/dpo_guideline)
- PPC 個人データの取扱いに関する責任者・責任部署の設置に関する事例集(2023 年11 月)(事例集)
- (https://www.ppc.go.jp/personalinfo/independent_effort/)

事例集の一部①

- 1 業務内容(個人データの取扱いに関する責任者等の責任(役割))
- 個人データの取扱いに関する責任者等の責任(役割)については、各事業者によって大きく異なるが、各事例によれば、以下のような責任を持つことがある。
 - ① 事業部門からの相談への対応や事業部門への助言
 - ② データ保護・プライバシー保護の観点からの事業の評価(PIA 等)
 - ③ データ保護・プライバシー・利活用に関わる施策・基準・規定等の策定・導入
 - ④ データの取扱状況の棚卸し及びリスク評価
 - ⑤ 外部の専門家(弁護士等)や経営層との相談・意見交換
 - ⑥ 社内教育

事例集の一部②

- 2 設置による効果
- 個人データの取扱いに関する責任者等の設置による効果としては、以下のようなものが挙げられる。
- ① データ保護・プライバシー保護の取組の推進
- ② 社内の相談窓口の明確化
- ③ 社内全体のデータ保護・プライバシー保護に関する意識の向上
- ④ 全社的な個人情報取扱いのルール等の見直し
- ⑤ 事業部門とは異なった視点による助言や経営層への報告

事例集の一部③

- 第4 事例集
- 本節では、A 社（サービス分野）、B 社（信用分野）、C 社（製造分野）、D 社（製薬分野）、E 社（通信分野）における個人データの取扱いに関する責任者及びその責任者を支える責任部署の概要（設置の背景、構成等）、業務内容、育成方法・人事評価制度及び設置による効果を紹介する（なお、今後必要に応じて事例を追加する場合がある。）。

UK Data Protection and Digital Information Bill 2023

- Data Protection and Digital Information Bill (18 July 2022)
- Data Protection and Digital Information (No.2) Bill (8 March 2023)
- Clause 15: Senior responsible individual
- 201. Clause 15 replaces the requirements on Data Protection Officers in Articles 37 to 39 of the UK GDPR and sections 69 to 71 of the DPA 2018. It introduces new requirements for controllers and processors to designate a “**senior responsible individual**” to be responsible for data protection risks within their organisations or delegate that task to suitably skilled individuals.

DPOからSRIへ

- Data Protection and Digital Information Bill in July 2022 で、data protection officer に代えて、senior responsible individual (SRI) を取り入れるという提案をした。この2022年法案は、首相の交替などもあり、成立しなかった。その後、2023年3月の同じタイトルのData Protection and Digital Information Bill (DPDI Bill) が提案された。2023年法案でも、SRIを取り入れることになっている。

SRI の任命

- An SRI must be appointed by an organisation that:
- (a) is a public body; or
- (b) carries out processing that is likely to result in a high risk to the rights and freedoms of individuals.
- Senior management
- SRI must be part of the organisation's senior management.
- SRIs cannot be appointed externally.
- 【Omitted below】