



データ保護責任者（DPO）を巡る 近時の動向と実務への示唆

～ 日本DPO協会 第23回個人情報保護セミナー～

自己紹介

◆ 生田美弥子

弁護士法人北浜法律事務所 東京事務所 パートナー



- 日本DPO協会顧問
- 日本（第二東京）、フランス、米国ニューヨーク州弁護士
- フランス（パリ）、ベトナム（ハノイ）、米国（ニューヨーク）、在東京
渉外系法律事務所での執務経験を経て現職
- 環境再生保全機構監事ほか、社外監査役等歴任
- GDPR対応を含む欧州関係の業務を担当

◆ 藤原成和

北浜法律事務所・外国法共同事業 アソシエイト

- 日本（大阪）弁護士
- 個人情報保護委員会事務局に出向（2022年1月～2023年12月）
- 出向では、G7データ保護・プライバシー機関ラウンドテーブル会合ほか、
国際業務を担当





CHAPTER 1

概説

CHAPTER 2

日本の動向

CONTENT

CHAPTER 3

EUの動向

CHAPTER 4

実務への示唆



CHAPTER 1
概説

CHAPTER 2
日本の動向

CONTENT

CHAPTER 3
EUの動向

CHAPTER 4
実務への示唆



CHAPTER1

概説（DPO） ～日EU制度の異同～

日EU制度の異同 (DPO)

	日本	EU
義務or任意	任意	義務 (一定の場合)
DPO人口	不明？ ※大企業向けアンケート調査では、88.6%が設置	登録者：70万人 (2023年IAPP)

DPO@EU

- 指名義務

- 3つの類型（体系的かつ大規模に個人を監視する場合等）いずれかに該当する場合
- ただし、任意の選任も可能

- 役割

- アカウンタビリティの礎
- 法令遵守の促進（ひいては競争上の優位獲得）

- 資格

- データ保護の法令及び実務に関する専門知識等

- 地位

- 個人データ保護に関するあらゆる問題に対する関与
- 必要なリソースの提供による支援
- 独立性、利益相反

- 任務

- GDPR遵守の監視 等

DPO@日本

個人情報保護に関する基本方針

- 根 拠：個人情報保護に関する法律第7条
- 目 的：個人情報保護に関する施策の総合的かつ一体的な推進
- 決定日：令和4年4月1日

④データガバナンス体制の構築

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。

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等が有効であり、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。

PIA等@日本

PIAの取組の促進について

個人情報保護委員会「PIAの取組の促進について—PIAの意義と実施手順に沿った留意点—」2021年6月30日
(https://www.ppc.go.jp/files/pdf/pia_promotion.pdf)

PIAを実施することを決定した場合は、PIAを実施するための体制を整備する必要がある。具体的には、**実施責任者の任命**、投入人員数などリソース計画、スケジュールの策定が挙げられる。

こうした準備にあたり、経営層がPIAの必要性等を理解・認識した上で、必要なリソースを割り当てることにコミットすることが重要である。

実施責任者については、事業者によって責任者の職位等のレベルは様々考えられるが、PIAの対象とする業務プロセスについての理解力とリスクの評価、対策の検討等に際しての適切な判断力を有する者である必要がある。

投入人員について、PIAは法令、システム面等様々な視点から評価を行う必要があるため、事業を実施する部門のみならず、法務部門やシステム部門等の人材も組み込みながら、責任者も含めて、評価者として数人程度のチームを組成することが考えられる。

なお、外部有識者も含む第三者機関を設置して、事案に応じて、チームが実施した評価及び検討した対応策について当該第三者機関が審議を行うといった方法も有効である。

所要期間については、最終的な事業の開始時期等を考慮する必要があるが、数週間から数か月程度での実施が考えられる。

事業の性質等によって適切な投入人数や所要期間が異なってくる点には留意が必要である。

データマッピング・ツールキット

個情委事務局「データマッピング・ツールキット（個人情報保護法関係）」2022年10月
(https://www.ppc.go.jp/files/pdf/data-mapping_tool-kit.pdf)

データマッピングの責任者・担当部署（事務局）を決定し、当該責任者・担当部署（事務局）がデータマッピングを取りまとめることにより、事業者内で統一的な考え方の下、データマッピングを行うことができます（担当部署としては、総務部門、法務部門、データ保護部門等が考えられます。）。

また、データマッピングのためには各部門の協力が不可欠です。そのため、データマッピング責任者は、各部門に対して実効的な協力要請ができる権限を有する者（役員等）であることが望ましいです。

日本プラクティスにおける法務・戦略的意義

- 安全管理措置義務（個人情報法第23条）
- 取締役の善管注意義務（会社法第330条、民法第644条等）
 - cf. 会社におけるサイバーセキュリティに関する体制（NISC等）
 - ✓ ただし、DPO設置・指名に関する具体的な法的義務はない。

◆ 狭義の法令遵守という観点...

→ 我が国におけるプラクティスには不要？

◆ 最低限のコンプライアンスで十分な事業・領域か？（リクナビ・Suica事件等）

→ “ベストプラクティス” という全社的戦略



CHAPTER 1

概説

CHAPTER 2

日本の動向

CONTENT

CHAPTER 3

欧州の動向

CHAPTER 4

実務への示唆



CHAPTER 1

概説

CHAPTER 2

日本の動向

CONTENT

CHAPTER 3

欧州の動向

CHAPTER 4

実務への示唆



CHAPTER2

日本のDPOに関する動向 ～PPC事例集～

本事例集 (※) の構成

(※) 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

1. 「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」
を公表する背景
2. 個人データの取扱いに関する責任者の個人情報保護法の位置付け
3. 各事例から分かる個人データの取扱いに関する責任者の実態
4. 事例集
 - A) サービス分野
 - B) 信用分野
 - C) 製造分野
 - D) 製薬分野
 - E) 通信分野

2. DPOの位置付け

個人情報取扱事業者は、個人情報保護法第 23 条に定める個人データの安全管理措置を講じなければならない。組織的安全管理措置として「組織体制の整備」を講じなければならない。その手法の一つとして「個人データの取扱いに関する責任者の設置及び責任の明確化」が挙げられる（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）10-3（1））。

全社横断的な個人データの取扱いに関する責任者を設置することにより、事業者内で統一した考え方で事業を実施することができるとともに社内の知見等が同責任者の下に集約することが期待される。事業者においては、本事例集で紹介された事例を参考にしつつ、個人データの取扱いに関する責任者を設置し、その責任を明確化するとともに、当該責任者が実効的な活動をする体制を整備することが望まれる。

→ **安全管理措置（組織的安全管理措置）？**

3. DPOの実態

1. 業務内容（役割）

- 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・利活用にかかわる施策・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

2. 設置による効果

- 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 全社的な個人情報の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

4. 事例集から

	地位	経歴	体制	育成	人事評価
A社	執行役員 (リスクマネジメント)	<ul style="list-style-type: none">事業部コーポレート部セキュリティ・法務	DPP部設置等 (弁護士、元エンジニア、マーケティング・渉外：20名超)	2週間の研修 <ul style="list-style-type: none">関連法令事業モデル、社内キーマン等のインプット	事業部門のKPIとは分離・独立して実施
B社	執行役員 (コンプライアンス)	<ul style="list-style-type: none">事業部リスク管理部	コンプライアンス部 情報管理室	<ul style="list-style-type: none">研修（個人情報・情報セキュリティ）SCM等での実務経験・学習	事業部と分離・独立して実施
C社	執行役員 (プライバシー)	<ul style="list-style-type: none">法務領域	本社法務 (コンプライアンス・プライバシー) 部門	<ul style="list-style-type: none">研修OJTでの工夫等	各活動の進捗等を基に総合的に実施
D社	執行役員 (General Counsel 兼 CCO)	<ul style="list-style-type: none">企業法務分野	法務部門 特に、専任の人員 (1名)	<ul style="list-style-type: none">研修OJTでの工夫等	CEO直属 (事業部・製造部から明確に分離)
E社	常務執行役員 (CDO)	<ul style="list-style-type: none">セキュリティ事業	CDO室	<ul style="list-style-type: none">研修OJTでの工夫等	事業部門と分離・独立して実施



CHAPTER 1

概説

CHAPTER 2

日本の動向

CONTENT

CHAPTER 3

EUの動向

CHAPTER 4

実務への示唆



CHAPTER 1

概説

CHAPTER 2

日本の動向

CONTENT

CHAPTER 3

EUの動向

CHAPTER 4

実務への示唆



CHAPTER3

EUのDPOに関する動向 ～EDPB協調的執行～

EDPB / 第2回CEF

CEFの概要

- 名称：協動的執行枠組み（Coordinated Enforcement Framework: CEF）
- 根拠：欧州データ保護委員会（EDPB）2021年～2023年の戦略－第2の柱
- 目的：
 - より効率的に機能するEU内当局間の協力・一貫性のあるメカニズムの確保
 - EU全域に及ぶ当局間の真の執行カルチャーの進展

第2回CEFの概要

- 対象：DPOの指定・地位 ※第1回は「公的機関によるクラウドサービスの利用」が対象
 - i. DPOが「新しいデータガバナンスシステムにおける重要なプレーヤー」であること等
 - ii. DPOが法とその適用の間のギャップを埋めること等
- 目的：DPOによる業務遂行における潜在的な困難の特定等
- 方法：以下の3段階による各国レベル（25機関）での実施
 - ① 事実調査
 - ② アンケートによる正式な調査の要否判断
 - ③ 正式な強制調査の開始・進行中の調査のフォローアップ
- 回答：1万7490（うち民間部門は1万2022）
- 成果：本活動による課題の特定

調査結果

項目	結果
インソース × アウトソース	<ul style="list-style-type: none"> インソース : 70%
所属部署	<ul style="list-style-type: none"> 最多=リーガル・コンプライアンス部門 : 34.6% 経営層 (?) : 約20% <ul style="list-style-type: none"> 最高経営陣 (Highest management) : 11.6% 経営管理 (Administrative management) : 9.2%
任意的DPOの指定	<ul style="list-style-type: none"> 任意によるDPO指名 : 約14%
専門性	<ul style="list-style-type: none"> 法務 : 63.89% ビジネスプロセス : 58.3% 情報セキュリティ : 39.3%
複数併任	<ul style="list-style-type: none"> 複数主体からのDPO指名 : 1/3以上

特定された課題

- ① DPO指定義務違反
- ② 割り当てられるリソース不足
- ③ 不十分な専門知識等
- ④ 重要な役割の非付与
- ⑤ 独立性欠缺等
- ⑥ 最高経営陣への報告欠缺
- ⑦ 監督当局の更なるガイダンス

②割り当てられるリソース不足

懸念点

- 人的資源（特に副DPO）の不足
 - 多忙による職務怠慢
 - 長期的なコンプライアンス維持の困難性
- 複数社のDPOを兼任する外部DPOのリソース不足

EDPB提言

- ✓ アウトソースでも原則問題なし
- ✓ 常勤のDPO + （任意的）副DPO
- ✓ DPO自身による自らの予算管理
- ✓ 会社による必要なリソースの分析・割当て
- ✓ 外部DPOの兼任調査

③不十分な専門知識等

懸念点

- データ保護法制の専門知識の必要性に関する認識されているか？
- 専門知識等獲得のためのトレーニングの不十分性
 - 25～32時間（年単位／以下同）：9.5%
 - ～24時間：24.7%
 - 0時間：4.3%

EDPB提言

- ✓ 組織的知見、訓練の必要性及び進捗等の文書化
- ✓ 外部研修の活用ほか、関連法制を含めた訓練の機会等確保

④重要な役割の非付与、⑤独立性欠缺等

- データ保護法に基づく義務に関する情報提供・助言：96.51%
- データ保護影響評価の実施状況の監視：69.66%
(1.75%は「わからない」又は「答えたくない」と回答)
- DPOの業務の文書化：83.57%
- 同文書の職員への周知：78.79%
 - ✓ DPAの役割について社内への周知徹底が必要
- DPIAのドラフト・実施：36.1%
- 処理に関する決定：20.7%
 - ✓ 十分な独立性（GDPR35条）の観点から懸念

cf. Case C-453/21, *X-FAB Dresden GmbH & Co. KG*



CHAPTER 1

概説

CHAPTER 2

日本の動向

CONTENT

CHAPTER 3

EUの動向

CHAPTER 4

実務への示唆



CHAPTER 1

概説

CHAPTER 2

日本の動向

CONTENT

CHAPTER 3

EUの動向

CHAPTER 4

実務への示唆



CHAPTER4

実務への示唆

ベストプラクティス

項目	ポイント
DPOの選定	<ul style="list-style-type: none"> • 個人情報に係る法務的知見（マスト） • 事業やセキュリティに関する知見（+） • アウトソースでもOK ※ただし、他社との兼務（-）
地位・職務	<ul style="list-style-type: none"> • 個人データ処理の目的・方法の決定（?） • 経営層への報告権限の欠缺（-） • 実態と内部規程との合致のウォッチング（+） • DPOの役割に関する社内周知・徹底（+） • 独立性
会社のサポート	<ul style="list-style-type: none"> • 副DPO設置（+） • トレーニング ※外部サービス含む ※年間25時間以上（+） • 予算付与（+）

課題（想定される論点）

- 兼職の適否
 - 役員等
 - 労働組合員（特に委員長等の代表者）
 - 公益通報対応業務従事者
- 懲戒権・損害賠償請求権制限の適否
 - 就業規則に「解任（等）されることがない」（GDPR38条3項）旨を定めた場合...？

DPO個人の損害賠償責任？

- EU

- 「職務の遂行に関して、...解任...又は罰則を受けることがない」 (第38条第3項)
- EDPB・ICO等の見解

- 日本

- 従業員 (民法第415条、709条、715条3項等)
 - 信義則 (最判昭和51年7月8日民集30巻7号689頁等)
 - cf. スルガ銀行事件に付随する元専務執行役員の労働訴訟等
- 役員等 (会社法第429条等)
 - 経営判断原則 (最判平成22年7月15日集民234号225頁等)

→ **(会社) 責任追及の実効性は低い**

(DPO) 重い義務 + 高いリスク ⇒ 萎縮効果？

→ **リスクの移転 (サイバーセキュリティ、D&O、E&O保険等)**

課題（想定される論点）

- 兼職の適否

- 役員等
- 労働組合員（特に委員長等の代表者）
- 公益通報対応業務従事者

- 懲戒権・損害賠償請求権制限の適否

- 就業規則に「解任（等）されることがない」（GDPR38条3項）旨を定めた場合...？
 - 特別に懲戒権等が限定？
- DPOの能力不足・不正（特に予算）への対応・予防

→ **ガバナンス等による予防＋リスク移転（保険活用）**



- 大阪 北浜法律事務所・外国法共同事業 (大阪)
〒541-0041 大阪市中央区北浜1丁目8番16号 大阪証券取引所ビル
TEL: 06-6202-1088 (代) / FAX: 06-6202-1080
- 東京 弁護士法人北浜法律事務所 東京事務所
〒100-0005 東京都千代田区丸の内一丁目7番12号 サピアタワー
TEL: 03-5219-5151 (代) / FAX: 03-5219-5155
- 福岡 弁護士法人北浜法律事務所 福岡事務所
〒812-0018 福岡市博多区住吉1丁目2番25号 キャナルシティ・ビジネスセンタービル4階
TEL: 092-263-9990 (代) / FAX: 092-263-9991