日本型DPIA実施要綱

牧野総合法律事務所弁護士法人

1　本書式の使用方法

我が国企業が EU 域内から個人データを取得し、利用するに当たり、GDPRの定めるところに従い、DPIA（データ保護影響評価）を実施しなければならないが、その参考とされるCNILの要求する書式では、我が国の実情、慣行と必ずしも整合しない点があることから、我が国ですでに実施されている「特定個人情報保護影響評価」による影響評価を基礎に置きつつ、さらにGDPRの要求事項（権利保護強化、業務記録の実施など）を追加し、かつ一般事業者において自己判断可能な形態とすることを目指した。

本書式は、個人データ全般について一括した記載をする方式ではなく、特定個人情報で採用されたファイル単位の保護影響評価を基礎とした。そのため、企業の取り扱う個人データの全容を把握した上で、その中でファイルとして統合され利用されるデータ毎の評価とした。したがって、対応ファイルが異なる度毎に、また新たなファイルが追加される毎に、同一の書式に定められた項目の検討を繰り返すこととなる。

本書のセキュリティについては、検討項目の特定はおこなったが、その評価にあたっては発生頻度、重要性についての個別判断が必要であり、検討項目毎の評価及び対応策の検討が必要となるため、慎重に検討されたい。不明な場合には、弊事務所に相談されたい。

以上の目的で作成されたものであることから、今後、EU及びその加盟国の監督機関からの要請で追加事項や具体化に対して変更、更新が行われることもあるので、注意されたい。

内容に関しては、各企業の特性を活かせるように、大きな枠組みとなっているため、具体的調査と評価に際しては、当方にご相談いただくか、専門家の助言を仰がれたい。

また、本書面は、管理者として実施することから、実施後のDPOないし、専門家の意見を聴取して、助言を仰ぐことが前提となることを確認されたい。

2　参考情報

本書面は、以下の情報を利用していることをあらかじめ確認ください。

① GDPRガイドライン：　DPIAガイドライン、DPOガイドライン、

② CNIL　説明資料　：　METHODOLOGY, PIA TEMPLATES

③ 特定個人情報保護影響評価　：　保護評価指針、保護評価指針の解説、別添記載要綱
国税庁保護評価報告書他

④ JISQ：　31000、31010、0073

DPIA調査報告書

1　取扱い概況（Overview of processing　）

1－1　管理者及び共同管理者、処理者の概要

1－2　取扱いデーター覧(全体概要)

1－3　取扱いデータのデータフロー(全体概要)

1－4　データ取扱いに関連する機器、プログラムの概要

2　対象とするデータ・ファイルの特定及び取扱い(データファイル毎の検討)

2－1　評価対象データ・ファイルの概要

① 取扱いデータ数

② 取扱いデータの種類、特性

③ 9条、10 条のデータの有無の判断

④ データを保管している装置の識別

2－2　利用目的

① 目的の記載

② 目的の正当性、的確性、具体性の検討

2－3　情報取得の合法性（§６　）

2－4　最小限原則（GDPR　§5c）

2－5　品質保持制度

2－6　保管期間の定めと点検

2－7　データファイルへの関与、移転等

① プロセッサ（情報処理事業者への委託）

② 企業グループ内での共同利用（前文 48 参照）

3　データ主体の権利保護

3－1　データ主体への情報提供（§13，14）

①開示内容

②開示方法

3－2　データポータビリティ権の確保、対処方法

3－3　開示請求、訂正請求、利用停止・消去、取扱い制限、異議の各請求権の確保、対処方法

3－4　各種請求権の周知、告知方法

3－5　委託先（処理者）との関係

① 委託する個人データの種類と取扱い目的

② 委託先選定基準

③ 委託先との契約関係

④ 委託先への監督状況

3－6　国際移転

① 国際移転する個人データの種類と取扱い目的

② 保護措置

③ 再移転の有無及び再移転についての保護措置

3－7　監督機関との事前協議の要否、その判断

4　データセキュリティの検討

4－1　データ収集段階

① 不適法な収集方法(詐欺、脅迫、窃取など)リスクと対応

② 情報提供義務の遂行

③ 本人同意なく収集リスクと対応

④ 過剰な収集（最小限原則違反）リスクと対応

⑤ 入手の際のデータ漏えいリスクと対応

4－2　データ内容の検討

① データ内容が最新であること

② データ内容が真実であること（過誤がないこと）

４－３　データ使用段階

①　利用目的外利用リスクと対応

②　無権限利用リスクと対応

③　無権限持ち出しリスクと対応

４－４　委託（処理者）

①　委託先による不正収集リスクと対応

②　委託先による目的外利用リスクと対応

③　委託先による保管にかかるリスクリスクと対応

④　委託先の不正消去、消去しないリスクと対応

⑤　契約終了後のデータ残存リスクと対応

⑥　再委託にかかるリスクと対応

４－５　データの提供、移転段階

①　不正な提供、移転のリスクと対応

②　不適切な方法による移転（移転システム、ツール）リスクと対応

③　誤ったデータの提供リスクと対応

④　誤った相手方への提供リスクと対応

４－６　ネットワークリスク

①　目的外入手リスクと対応

②　安全性のない入手リスクと対応

③　不正確な情報の入手リスクと対応

④　入手時の漏えいリスクと対応

⑤　不正提供リスクと対応

⑥　漏えいリスクリスクと対応

⑦　誤った情報の提供リスクと対応

⑧　誤った相手への提供リスクと対応

４－７　保管段階のリスク

①　漏えいの危険

物理的漏えいリスクと対応

システム上の漏えいリスクと対応

②　消去、改竄の危険

人的介入リスクと対応

物理的障害リスクと対応

システム的リスクと対応

③ 所在不明（利用できない）

④ バックアップ体制

バックアップの確保

バックアップのミスの発生（システムバグなど）リスクと対応

⑤ システム障害（利用障害）

電源遮断リスクと対応

自然障害リスクと対応

４－８ 消去段階のリスク

① 保管期間経過による消去の手続きと制度的確立

② 誤消去リスクと対応

③ 消去しないリスクと対応

④ バックアップからの消去リスクと対応

５ 記録確保

① 同意確保とその記録

② 主要な業務の記録

６ 専門家等意見聴取について

① 専門家意見

② データ主体の意見（必要に応じて）

③ 企業方針との調整、検討結果