GDPR条項と類似する日本法令

※GDPR該当条項が公的機関に適用されるかとは無関係に、個情法・行個法等の日本法で類似するものを記載。主に個情法を中心に上げ、補足的に行個法等を記載している。
※ミス・漏れ等もあるため、使用する際は再度の確認が必要

GDPR		内容	義務者	類似する日本法
5		個人データの取扱いに関する基本原則	基本的に限定無	
5I	(a)	適法性・公正性・透明性	基本的に限定無	不法行為（プライバシー権侵害）で対応 個情法17Iは適正取得
5I	(b)	目的の限定	基本的に限定無	個情法15I, 16,17I
5I	(c)	データ最小化	基本的に限定無	不法行為（プライバシー権侵害）で対応 行個法3I, 3II
5I	(d)	正確化	基本的に限定無	個情法19（正確化の努め） 行個法5（正確化の努め）
5I	(e)	保存制限	基本的に限定無	個情法19（削除） 行個法3II（保有制限）
5I	(f)	完全性・機密性	基本的に限定無	個情法20（安全管理措置） 行個法6I（安全管理措置）
5II		アカウンタビリティ	管理者	黙示のルールとして対応
6I		いずれかに当たる取扱いが適法	基本的に限定無	個情法16に類似 行個法8に類似
6I	(a)	同意	基本的に限定無	個情法16I 行個法8II①
6I	(b)	契約履行等	基本的に限定無	個情法16I（目的内取扱い） 行個法8I（目的内利用・提供）
6I	(c)	法的義務遵守に必要	基本的に限定無	個情法16III①（法令に基づく目的外取扱い）
6I	(d)	生命保護に必要	基本的に限定無	個情法16III②（生命・身体・財産保護のための目的外取扱い） 行個法8II②（所掌事務のための目的外利用・提供）、8II④（本人利益のための目的外提供）
6I	(e)	公共の利益又は公的権限行使のために必要	基本的に限定無	個情法16III①（法令に基づく目的外取扱い）、16III③（公衆衛生等のための目的外取扱い）、16III④（国等への協力のための目的外取扱い） 行個法8II②（所掌事務のための目的外利用）、8II③（他の機関の所掌事務のための目的外提供）、8II④（統計・本人利益・特別理由のための目的外提供）

	6I	(f)	正当な利益のために必要（限定あり）	基本的に限定無	個情法16I・16III 行個法8I・8II
	6II		加盟国による6I(c)(e)条項	–	–
	6III		6I(c)(e)の根拠	–	–
	6IV		目的外利用	管理者	
	6IV	(a)	関連性	管理者	個情法16II（利用目的の変更要件） 行個法3III（利用目的の変更要件）
	6IV	(b)	収集経緯	管理者	不法行為（プライバシー権侵害）で対応
	6IV	(c)	性質（センシティブ性）	管理者	個情法17IIに若干類似
	6IV	(d)	発生しうる結果	管理者	不法行為（プライバシー権侵害）で対応
	6IV	(e)	保護措置（暗号化・仮名化等）	管理者	個情法20（安全管理措置）に類似 行個法6I（安全管理措置）に類似
7			同意の要件としての証明		
	7I		同意の要件としての証明	管理者	ガイドラインで推奨
	7II		同意の明確性（区別・平易等）	（管理者）	ガイドラインで推奨
	7III		撤回権利	（管理者）	人を対象とする医学系研究に関する倫理指針等では
	7IV		同意の任意性（契約履行に必要か等）	（管理者）	–
8			子どもの同意に適用される要件		
	8I		16才以上の同意は適法。16才未満は親権者等の同意等が必要。加盟国は年齢を引き下げることも可。	基本的に限定無	ガイドラインで未成年者は親権者の同意要
	8II		親権者等の同意等の確認の努め	管理者	–
	8III		子どもとの契約法へは無影響	–	–
9			特別な種類の個人データ		
	9I		データ取扱いの禁止(racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, bilmetric data, health, sex life, sexual orientation)	基本的に限定無	個情法17II（要配慮個人情報の取得制限）に類似 個人情報保護条例によっては機微情報取扱制限規定あり
	9II		以下の場合は取り扱える	基本的に限定無	
	9II	(a)	明確な同意	基本的に限定無	個情法17II
	9II	(b)	法が認める範囲内、団体協約が認める範囲内で雇用・社会保障・社会的保護の法律義務履行、特別の権利行使	基本的に限定無	個情法17II①
	9II	(c)	同意困難で生命保護のため	基本的に限定無	個情法17II②
	9II	(d)	政治、宗教団体等が構成員等のデータを同意なく外部に開示されないことを条件として取	基本的に限定無	–
	9II	(e)	本人が公開	基本的に限定無	個情法17II⑤
	9II	(f)	訴訟関係	基本的に限定無	個情法17II①

9II	(g)	重要な公益実現に必要等	基本的に限定無	個情法17II①③④
9II	(h)	医療等	基本的に限定無	個情法17II①②
9II	(i)	公衆衛生	基本的に限定無	個情法17II③
9II	(j)	公益・研究・統計目的の保管	基本的に限定無	個情法17II①④
9III		守秘義務者による9II(h)	基本的に限定無	–
9IV		加盟国による遺伝子データ等の条件付加	–	–
10		犯罪関連データの取扱い	基本的に限定無	個情法17II①④
11		識別を要しない取扱い	管理者	–
11I		識別のための情報保管は義務付けられない	管理者	
11II		本人通知	管理者	
12		本人への情報提供等	管理者	
12I		アクセス権保障等のための理解しやすい措	管理者	個情法27
12II		アクセス権行使等を容易にする	管理者	個人情報保護条例によっては見られる、個情法32IV
12III		アクセス権行使時の遅滞ない連絡等	管理者	個情法28II・III等、行個法19・20等
12IV		アクセス権行使時の遅滞ない連絡等（不開示等）	管理者	
12V		無償での実施	管理者	–
12V	(a)	有償での実施の例外	管理者	個情法33、行個法26（日本法は有償が原則）
12V	(b)	拒否の例外	管理者	–
12VI		アクセス時の身元確認	管理者	行個法13I・II
12VII		標準的なアイコンの提供	管理者	–
12VIII		欧州委員会	–	–
13		本人からの取得	管理者	
13I		以下の全ての情報提供義務	管理者	
13I	(a)	身元・連絡先	管理者	個情法27I①
13I	(b)	データ保護オフィサーの連絡先	管理者	–
13I	(c)	利用目的・法的根拠	管理者	個情法27I②
13I	(d)	6I(f)の場合の正当な利益	管理者	–
13I	(e)	個人データの取得者・取得者類型	管理者	行個法11・10I⑥
13I	(f)	第三国提供の事実等	管理者	–
13II		必要な以下の情報を提供	管理者	
13II	(a)	保存期間等	管理者	–
13II	(b)	アクセス権の存在	管理者	個情法27I③
13II	(c)	同意撤回	管理者	人を対象とする医学系研究に関する倫理指針等では
13II	(d)	監督機関に異議を申し立てる権利	管理者	–
13II	(e)	個人データの提供が法又は契約上の要件か、契約締結に必要な要件か、提供義務を負うか、提供しないとどうなるか	管理者	–
13II	(f)	プロファイリング等	管理者	–

	13III		目的外利用の場合、事前に13IIを情報提供	管理者	−
	13IV		本人既知時には適用外	管理者	−
14			本人以外からの取得	管理者	
	14I			管理者	
	14I	(a)	身元・連絡先	管理者	個情法27I①
	14I	(b)	データ保護オフィサーの連絡先	管理者	−
	14I	(c)	利用目的・法的根拠	管理者	個情法27I②
	14I	(d)	個人データの種類	管理者	行個法11・10I④
	14I	(e)	個人データの取得者・取得者類型	管理者	行個法11・10I⑥
	14I	(f)	第三国提供の事実等	管理者	−
	14II		必要な以下の情報を提供	管理者	
	14II	(a)	保存期間等	管理者	−
	14II	(b)	6I(f)の場合の正当な利益	管理者	
	14II	(c)	アクセス権の存在	管理者	個情法27I③
	14II	(d)	同意撤回	管理者	人を対象とする医学系研究に関する倫理指針等では
	14II	(e)	監督機関に異議を申し立てる権利	管理者	−
	14II	(f)	情報源	管理者	−
	14II	(g)	プロファイリング等	管理者	−
	14III		情報提供方法等	管理者	個情法27・18
	14III	(a)	合理的な期間内（1カ月内）	管理者	
	14III	(b)	最初の連絡時	管理者	
	14III	(c)	提供前	管理者	
	14IV		目的外利用の場合、事前に13IIを情報提供	管理者	−
	14V		以下の場合は適用外	管理者	
	14V	(a)	本人既知時	管理者	個情法18IV④
	14V	(b)	公益・研究・統計目的達成が不可能等	管理者	個情法18IV③
	14V	(c)	加盟国法等により明示されている場合	管理者	−
	14V	(d)	守秘義務	管理者	個情法18IV①
15			アクセス権	管理者	
	15I	(a)	取扱目的	管理者	個情法27・18
	15I	(b)	個人データの種類	管理者	−
	15I	(c)	取得者・取得者の類型、特に第三国等の取	管理者	−
	15I	(d)	保存期間等	管理者	−
	15I	(e)	アクセス権の存在	管理者	個情法27I③
	15I	(f)	監督機関に異議を申し立てる権利	管理者	−
	15I	(g)	情報源	管理者	−
	15I	(h)	プロファイリング等	管理者	−
	15II		本人通知	管理者・処理者	−
	15III		開示（有償）	管理者	個情法28

15IV		開示による他の者の権利保護	–	個情法28II①
16		不正確な個人データの訂正	管理者	個情法29
17		忘れられる権利	管理者	
17I		消去義務	管理者	
17I	(a)	目的上不要	管理者	個情法19、行個法3II
17I	(b)	同意撤回し法的根拠が他にない	管理者	–
17I	(c)	異議	管理者	–
17I	(d)	違法に取り扱われた	管理者	個情法30
17I	(e)	法的義務遵守のために消去必要	管理者	–
17I	(f)	8I子供の情報社会サービス提供に関して収	管理者	–
17II		消去義務を負っているデータを公開している場合、合理的な手立て	管理者	–
17III		以下の場合適用外	管理者	
17III	(a)	表現の自由等	管理者	個情法76I
17III	(b)	法的義務遵守等のため	管理者	–
17III	(c)	9II(h)(i),9III公衆衛生のため	管理者	–
17III	(d)	89I公益・研究・統計	管理者	–
17III	(e)	訴訟関係	管理者	–
18		取扱い制限を得る権利	管理者	
18I		正確性疑義がある場合、正確性を確認する期間内	管理者	–
18I	(a)	違法取扱、かつ本人が消去に反対	管理者	個情法30
18I	(b)	管理者は不要だが、本人が訴訟関係で必要	管理者	–
18I	(c)	管理者の正当性根拠が本人の正当性根拠より優先するか争い、異議	管理者	–
18II		18Iによる取扱い制限時の処理	管理者	–
18III		本人通知	管理者	–
19		訂正・消去・取扱い制限の通知	管理者	個情法27-32
20		データポータビリティ	管理者	–
20I		以下の両要件を満たす場合に可	管理者	–
20I	(a)	6I(a),9II(a)による同意、6I(b)による契約、かつ	管理者	–
20I	(b)	自動化手段	管理者	–
20II		直接移転	管理者	–
20III		データポータビリティは忘れられる権利を妨げない	_	–
20IV		他の者の権利保護	–	–
21		異議を述べる権利		–

	21I	6I(e)(f)の取扱い及びプロファイリングに異議を述べる権利。管理者は、本人の権利等より優先する取扱い又は訴訟関係についてやむを得ない正当な根拠を証明しない限り、以後	管理者	–
	21II	ダイレクトマーケティングに異議を述べる権利	基本的に限定無	–
	21III	前項の場合、ダイレクトマーケティング目的の取扱禁止	基本的に限定無	–
	21IV	本人に異議権を明示的に表示する義務	基本的に限定無	–
	21V	自動化手段	–	–
	21VI	公益・研究・統計の場合の異議	基本的に限定無	–
22		プロファイリング等		–
	22I	自動化された取扱いに基づいた決定の対象とされない権利	基本的に限定無	–
	22II	以下のいずれかの場合には適用外	基本的に限定無	–
	(a)	契約のために必要	管理者	–
	(b)	法によって認められる場合	管理者	–
	(c)	同意	基本的に限定無	–
	22III	22II(a)(c)では適切な措置要	管理者	–
	22IV	9II(a)(g)かつ適切な措置の場合を除き、9I特別な種類のデータを基礎としてはならない	基本的に限定無	–
23		制限	–	–
	23I	国内法等による12-22、34、5の制限可((a)～(j)を保護するために必要・比例的な措置)	–	–
	23II	23Iは(a)～(h)までの特別条項を含める	–	–
24		管理者の責任	管理者	
	24I	リスクを考慮し、GDPRに沿って取り扱い、それを証明できるよう技術上・組織上の措置を実装しPDCA	管理者	個情法全体・20
	24II	データ保護方針の実装	管理者	ガイドラインで推奨
	24III	40行動規範、42認証方法は、義務履行を証明する要素として使える	管理者	–
25		データ保護バイデザイン・データ保護バイデフォルト	管理者	–
	25I	データ保護の基本原則の実装、技術的措置・組織的措置	管理者	–
	25II	目的達成に必要な個人データのみ取り扱う	管理者	–
		40行動規範、42認証方法は、義務履行を証明する要素として使える	管理者	–
26		共同管理者	管理者	–

26I		共同管理者同士で合意で責任を定める	管理者	–
26II		合意に役割・関係を反映	管理者	–
26III		本人が自己の権利行使可	管理者	–
27		EU域内に拠点のない管理者又は処理者の代理人	管理者・処理者	–
27I		3IIの場合、書面により代理人指定	管理者・処理者	–
27II		以下の場合適用外	管理者・処理者	–
	(a)	一時的、特別な種類のデータを大量に含まず、リスク低い	管理者・処理者	–
	(b)	公	管理者・処理者	–
27III		本人がいる加盟国の一つに設ける	管理者・処理者	–
27IV		特に監督機関及び本人対応	管理者・処理者	–
27V		訴訟行為	–	–
28		処理者		
28I		GDPR適合態様で技術上・組織上の保護措置を実装する処理者を用いる	管理者	個情法22
28II		承認のない別の処理者の制限	処理者	マイナンバー法10I
28III		契約等による規律	処理者	ガイドライン
	(a)	管理者からの文書指示	処理者	–
	(b)	守秘義務を課す	処理者	–
	(c)	32(Security of processing)のすべての措置を講じる	処理者	ガイドライン
	(d)	別の処理者には28II・IVを尊重	処理者	–
	(e)	技術上・組織上の措置で管理者支援	処理者	–
	(f)	32-36で管理者支援	処理者	–
	(g)	消去	処理者	–
	(h)	監査受け入れ	処理者	ガイドライン
28IV		別の処理者を用いる場合	処理者	–
28V		40行動規範、42認証方法は、義務履行を証明する要素として使える	処理者	–
28VI		標準契約条項に基づくことが可	処理者	–
28VII		欧州委員会	–	–
28VIII		監督機関	–	–
28IX		書面、電子的による契約等	–	–
28X		処理者は管理者として扱われる	処理者	個情法の個人情報取扱事業者概念
29		管理者からの指示がない限り取扱い禁止	処理者、管理者及び処理者権限の下の行為	–
30		取扱活動の記録		ガイドライン
30I		以下を含めた記録保管。	管理者(管理者代理	–

	(a)	管理者の名前・連絡先等	管理者（管理者代理	–
	(b)	取扱い目的	管理者（管理者代理	–
	(c)	本人の類型、個人データの種類	管理者（管理者代理	–
	(d)	取得者の類型（第三国等含む）	管理者（管理者代理	–
	(e)	第三国等への移転の場合適切な保護措置を示す文書	管理者（管理者代理人）	–
	(f)	データ削除のために予定されている期限	管理者（管理者代理	–
	(g)	技術的・組織的措置	管理者（管理者代理	–
30II		以下を含めた記録保管。	処理者（処理者代理	ガイドライン
	(a)	処理者の名前・連絡先等	処理者（処理者代理	–
	(b)	取扱いの種類	処理者（処理者代理	–
	(c)	第三国等への移転の場合適切な保護措置を示す文書	処理者（処理者代理人）	–
	(d)	技術的・組織的措置	処理者（処理者代理	–
30III		書面、電子	管理者（管理者代理人）・処理者（処理者代	–
30IV		監督機関が記録を利用できるようにする	管理者（管理者代理人）・処理者（処理者代	–
30V		従業者数250人以下の非適用	管理者・処理者	ガイドラインの中小規模事業者
31		監督機関との協力	管理者（管理者代理人）・処理者（処理者代	
32		取扱いの安全性		
32I		技術上・組織上の措置（特に以下）	管理者・処理者	個情法20
	(a)	仮名化・暗号化	管理者・処理者	–
	(b)	機密性・完全性・可用性・回復性確保	管理者・処理者	–
	(c)	復旧力	管理者・処理者	–
	(d)	テスト、評価	管理者・処理者	–
32II		破壊、喪失、改変、無権限開示又はアクセスから生じるリスクの考慮	管理者・処理者	個情法20
32III		40行動規範、42認証方法は、義務履行を証明する要素として使える	–	–
32IV		従業者の適法性確保	管理者・処理者	個情法21
33		漏えい等の通知（監督機関）		△告示
33I		72時間以内の監督機関への通知	管理者	△告示
33II		管理者への通知	処理者	–
33III		33Iの通知方法	管理者	
	(a)	本人類型・概数、データ種類・概数、侵害の性	管理者	△告示
	(b)	データ保護オフィサーの連絡先等	管理者	–
	(c)	発生しうる結果	管理者	△告示

(d)	対応	管理者	△告示
33IV	五月雨通知可	管理者・処理者	−
33V	文書化	管理者	△告示
34	漏えい等の通知（本人）		
34I	本人通知	管理者	△告示
34II	明瞭・平易、通知事項	管理者	−
34III	以下の場合適用外	管理者	−
(a)	技術上・組織上保護措置を実装していて、無権限者は識別不可	管理者	−
(b)	リスク具体化防止策を講じた場合	管理者	−
(c)	過大な負担になる場合	管理者	−
34IV	本人通知していない場合の監督機関の要求	−	−
35	データ保護影響評価		マイナンバー法28
35I	高リスク時はDPIA実施義務	管理者	
35II	データ保護オフィサーの助言	管理者	
35III	特に以下の場合に求められる	管理者	
(a)	プロファイリング等	管理者	
(b)	9I特別な種類のデータ、10犯罪	管理者	
(c)	公衆アクセス可能な大規模システム監視	管理者	
35IV	監督機関のリスト作成義務	−	
35V	監督機関の不要リスト作成	−	
35VI	監督機関の63一貫性メカニズム	−	
35VII	評価事項	管理者	
(a)	体系的記述（正当な利益）	管理者	
(b)	必要性・比例性	管理者	
(c)	リスク評価	管理者	
(d)	保護措置等	管理者	
35VIII	40行動規範、42認証方法は、義務履行を証明する要素として使える	−	−
35IX	本人等からの意見聴取	管理者	
35X	6I(c)(e)で法根拠があるなどした場合の義務	管理者	
35XI	評価の見直し	管理者	
36	事前協議		
36I	高リスク時の監督機関との協議	管理者	−
36II	監督機関による助言	−	−
36III	管理者による監督機関への情報提供	管理者	個情法40I
36IV	加盟国の監督機関との協議	−	−
36V	国内法	−	−
37	データ保護オフィサー	管理者・処理者	ガイドライン上の責任者

37I		以下の場合の指名義務	管理者・処理者	–
	(a)	公	管理者・処理者	–
	(b)	大規模監視	管理者・処理者	–
	(c)	9I特別な種類のデータ、10犯罪	管理者・処理者	–
37II		企業グループによる1名の指名	管理者・処理者	–
37III		公の場合の1名の指名	管理者・処理者	–
37IV		データ保護オフィサーを指名できる	管理者・処理者	–
37V		データ保護オフィサーの要件	管理者・処理者	–
37VI		データ保護オフィサーの資格	管理者・処理者	–
37VII		データ保護オフィサーの連絡先	管理者・処理者	–
38		データ保護オフィサーの地位		–
38I		全問題への関与	管理者・処理者	–
38II		データ保護オフィサーへの支援	管理者・処理者	–
38III		データ保護オフィサーの独立性	管理者・処理者	–
38IV		本人はデータ保護オフィサーと連絡できる	–	–
38V		秘密保持	データ保護オフィサー	–
38VI		兼業可	データ保護オフィサー	–
39		データ保護オフィサーの職務	データ保護オフィサー	–
39I		少なくとも以下の職務を行う	データ保護オフィサー	–
	(a)	義務通知・助言	データ保護オフィサー	–
	(b)	訓練・監査・コンプラ等	データ保護オフィサー	–
	(c)	DPIAへの助言・監視	データ保護オフィサー	–
	(d)	監督機関との協力	データ保護オフィサー	–
	(e)	監督機関の連絡先として行動	データ保護オフィサー	–
39II		リスクに注意を払う	データ保護オフィサー	–
40		行動規範Codes of conduct		–
40I		加盟国等による行動規範作成奨励	–	–
40II		行動規範の用意・追補	管理者・処理者を代表する団体等	認定個人情報保護団体に若干類似
	(a)	公正・透明性		–
	(b)	正当な利益		–
	(c)	収集		–
	(d)	仮名化		–
	(e)	公衆及び本人に提供される情報		–
	(f)	本人の権利行使		–
	(g)	子ども		–
	(h)	24.25.32		–
	(i)	漏えい等の通知		–
	(j)	第三国等への移転		–

	(k)	77,79を妨げることない紛争解決手段		–
40III		46II(e)データ移転によって3適用対象外の者にも遵守要。拘束力・執行性のある約束形成	移転者	–
40IV		監視	行動規範に従う者	–
40V		改正等	管理者・処理者を代表する団体等	–
40VI		監督機関による登録・公表	–	–
40VII		欧州データ保護会議	–	–
40VIII		欧州データ保護会議	–	–
40IX		欧州委員会	–	–
40X		欧州委員会による周知	–	–
40XI		欧州委員会による整理列挙	–	–
41		承認された行動規範の監視		–
41I		行動規範遵守の監視は、認定組織によって行われ得る	–	認定個人情報保護団体に若干類似
41II		組織認定の要件	–	–
	(a)	独立性・専門性の証明	–	–
	(b)	手続	–	–
	(c)	苦情対応手続・組織	–	–
	(d)	利益相反発生せず	–	–
41III		63一貫性メカニズムによって認定基準案を送	–	–
41IV		違反時の対応	–	–
41V		認定取消	–	–
41VI		適用除外	–	–
42		認証		–
42I		認証取得の奨励	–	–
42II		46II(f)データ移転によって3適用対象外の者の保護措置を示す目的で、マークを設けることができる。	–	–
42III		透明な手続	–	–
42IV		認証は責務を軽減しない	–	–
42V		欧州データ保護シール	–	–
42VI		監督機関への情報提供	–	–
42VII		最長3年、取消も	–	–
42VIII		欧州データ保護会議による整理列挙	–	–
43		認証機関	–	–
43I		加盟国は以下から認証を確保	–	–
	(a)	監督機関	–	–
	(b)	国内認定機関	–	–

	43II	認定要件	–	–
	(a)	独立性・専門性の証明	–	–
	(b)	監督機関等による承認	–	–
	(c)	手続	–	–
	(d)	苦情対応手続・組織	–	–
	(e)	利益相反発生せず	–	–
	43III	承認基準	–	–
	43IV	認証評価の責任	–	–
	43V	認証付与・取消の情報提供	–	–
	43VI	基準のアクセス	–	–
	43VII	取消	–	–
	43VIII	委任法令	–	–
	43IX	実装法令	–	–
44		移転に関する第5章遵守	移転者	個情法26
45	45I	十分制認定に基づく移転	移転者	個情法26
	45II	十分性評価の要素	–	
	(a)	法	–	
	(b)	独立の監督機関	–	
	(c)	国際的取り決め	–	
	45III	欧州委員会による決定	–	
	45IV	欧州委員会による監視	–	
	45V	欧州委員会による監視による取消	–	
	45VI	欧州委員会による協議	–	
	45VII	46-49の適用	–	
	45VIII	欧州委員会による公表	–	
	45IX	経過措置	–	
46		適切な保護措置に従った移転	–	個情法26
	46I	適切な保護措置・執行可能な権利及び司法救済の利用可能性による個人データ移転	移転者	
	46II	監督機関から個別の承認は不要で、以下のいずれかの保護措置が必要	移転者	
	(a)	公的機関等の法的拘束力及び執行力のある文書化	移転者	
	(b)	47拘束的企業準則	移転者	
	(c)	93II審判手続きに従って欧州委員会に採択された標準データ保護条項	移転者	
	(d)	監督機関によって採択され93II審判手続きに従って欧州委員会に承認された標準データ保護条項	移転者	

	(e)	40行動規範	移転者	
	(f)	42認証方法	移転者	
46III		監督機関から承認を得れば、以下の方法による保護措置も可	移転者	
	(a)	契約条項	移転者	
	(b)	執行可能かつ効果的な権利を含む条項	移転者	
46IV		63一貫性メカニズム	–	
46V		経過措置	–	
47		拘束的企業準則Binding coporate rules		個情法26
47I		次の場合の監督機関による承認	–	
	(a)	企業グループ等	–	
	(b)	執行可能な権利及び取扱いの明示	–	
	(c)	47II要件	–	
47II		少なくとも以下の事項を明記	移転者	
	(a)	組織体制・連絡先	移転者	
	(b)	個人データの種類、取扱種類、目的、本人類型、移転	移転者	
	(c)	法的性質	移転者	
	(d)	一般的なデータ保護原則の適用	移転者	
	(e)	権利	移転者	
	(f)	加盟国に拠点のある管理者・処理者の承諾	移転者	
	(g)	本人への情報提供等	移転者	
	(h)	データ保護オフィサー等	移転者	
	(i)	異議申立て	移転者	
	(j)	遵守確認方法	移転者	
	(k)	変更報告等	移転者	
	(l)	監督機関との協力の仕組み	移転者	
	(m)	悪影響を及ぼす法律上の要件を報告する仕	移転者	
	(n)	データ保護トレーニング	移転者	
47III		欧州委員会	–	
48		EU法によって認められていない移転・開示	管理者・処理者	
49		特定の状況における例外	移転者	
49I		十分性認定がなく、46保護措置がない場合でも、以下なら移転可	移転者	
	(a)	リスク提示後の同意	移転者	個情法26
	(b)	契約	移転者	
	(c)	本人利益のための契約	移転者	
	(d)	公共の利益の重大な事由	移転者	
	(e)	同意困難で生命保護のため	移転者	

(f)	法	移転者	
	正当な利益、評価、保護措置	移転者	
49II	49I(g)	移転者	
49III	49I(a)(b)(c)	移転者	
49IV	49I(d)	移転者	
49V	EU法・国内法	移転者	
49VI	文書化	管理者・処理者	
50	個人データ保護のための国際協力		個情法61⑥
51-59	独立監督機関		個情法59-78
60-76	協力と一貫性		
77	監督機関に異議を申し立てる権利	管理者・処理者等	
78	監督機関を相手方とする司法救済	-	
79	管理者又は処理者を相手方とする司法救済	管理者・処理者	
80	本人の代理人	-	
81	訴訟手続の停止	-	
82	賠償の権利及び法的責任	管理者・処理者	
83	制裁金を科すための一般的要件	管理者・処理者等	
84	制裁	管理者・処理者等	
85	表現の自由等		個情法76I
86	公文書		
87	国民識別番号		マイナンバー法
88	雇用		
89	公益・研究・統計目的		
90	守秘義務		
91	教会等		

委託関係のGDPRと日本の個人情報保護法との対比

※GDPRと日本の個人情報保護法で単純な比較はできない（∵規制の性質・対象・範囲等が異なる場合も多い）が、参照用の便宜として、委託についてGDPRと日本の個人情報保護法について、簡便な対比を行うもの。
※ミス・漏れ等もあるため、使用する際は再度の確認が必要

トピック	GDPR		日本の個人情報保護法	
委託元	委託という概念ではなく、Controller概念（自然人又は法人、公的機関、部局又はその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者）。 また、Controllerでなくても生じる義務あり。もっとも、純粋に私的な行為又は家庭内の行為の過程における自然人による個人データの取扱いであって、職業活動又は商業活動とは何らの関係もないものには適用されない（前文18）。	2条7項	個人情報取扱事業者が規制対象であり、個人情報取扱事業者として、委託先の監督責任を負う。個人情報取扱事業者でない場合は、基本的には民法上の不法行為責任のみ。 なお、個人情報取扱事業者とは、平たくいうと、検索できる体系的な個人データを事業に使っている者のこと。	2条5項、22条
委託先	委託という概念ではなく、Processor概念（管理者の代わりに個人データを取扱う自然人若しくは法人、公的機関、部局又はその他の組織）。 Controllerを規制対象とするGDPR上の義務は課せられない。 なお、Processorとは異なる概念として、共同管理者（Joint Controller、二者以上の管理者が共同して取扱いの目的及び方法を決定する場合）という概念もある。 さらに委託先とはかなり異なる概念として、代理人という概念もある（Representative、EU域内における代理人のこと）。	2条8項、26条、27条、28条（特に28条10項）	個人情報取扱事業者が規制対象であり、個人情報取扱事業者として各種義務を果たす責任を負う。個人情報取扱事業者でない場合は、基本的には民法上の不法行為・契約責任のみ。	2条5項、22条
再委託	事前の書面承認が必要。かつ、ProcessorはControllerがProcessorを監督するように、再委託に関してはControllerが果たすべき28条1・3項義務を負う。	28条2・4項	マイナンバー法、次世代医療基盤法以外は、基本的に再委託規制はない。しかし契約慣行によって許諾制を課す例も多い。	22条
委託に関する規制（概観）	GDPRに定める義務に適合するような態様で適切な技術上及び組織上の保護措置を実装することについて十分な保証を提供する処理者のみを用いるものとし、かつ、データ主体の権利の保護を確保する。 なお、この「保証」として、GDPR40条のApproved code of conductやGDPR42条のApproved certificationを用いることができる。	28条1・5項	個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。 ガイドラインで、委託先の選定、委託契約、委託先における取扱状況の把握が求められる。	22条

委託契約	以下を定める ・取扱いの対象及び期間（subject-matter and duration of the processing） ・取扱いの性質及び目的（nature and purpose of the processing） ・個人データの種類及びデータ主体の類型 ・管理者の義務及び権利 ・管理者からの文書化された指示のみに基づいて個人データを取扱うこと。指示がGDPR等に違反する場合直ちに管理者に通知すること。 ・守秘義務 ・32条（Security of Processing）によって求められるすべての措置を講ずること ・再委託規制（GDPR28条2・4項）の要件を遵守すること ・GDPR3章の本人権利のための管理者義務を踏まえ管理者を支援すること（細かい修飾語がほかにあり） ・GDPR32-36条（Security of Processing、Data Breach、DPIA）に関する管理者義務を踏まえ管理者を支援すること（細かい修飾語がほかにあり） ・サービス終了時の消去・返却、複製物の消去（細かい修飾語がほかにあり） ・監査 なお、欧州委員会は、標準契約条項を定めることができる（→見当たらない？）	28条3・7・8項、29条	以下を盛り込むことが望ましい。 ・必要かつ適切な安全管理措置の内容 ・委託先における委託された個人データの取扱状況を委託元が合理的に把握すること	ガイドライン43頁

GDPR関連資料

・前文日本語仮訳　https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf

・条文日本語仮訳　https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

・その他ガイドライン等の日本語仮訳　https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/

・GDPRと類似する日本法令（水町作成資料）　https://www.miyauchi-law.com/f/181105GDPRandJapaneseActs.pdf

・GDPR日本語仮訳の要修正点（水町ブログ）　https://cyberlawissues.hatenablog.com/entry/2019/04/02/100223?_ga=2.99631388.324283242.1554094963-223670487.1399716393

・Data Protection Officer（DPO）まとめ（水町ブログ）　https://cyberlawissues.hatenablog.com/entry/2019/03/19/095048

・顔認証と顔画像（水町ブログ）https://cyberlawissues.hatenablog.com/entry/2019/05/14/090430

GDPRと日本法の要配慮個人情報の比較

※ミス・漏れ等もあるため、使用する際は再度の確認が必要

要配慮個人情報			special categories of personal data（GDPR9）
人種	本人の人種（法2条3項）	例）アイヌ	racial or ethnic origin
信条	信条（法2条3項）	例）政治的思想	political opinions, religious or philosophical beliefs
社会的身分	社会的身分（法2条3項）		
障害・健康等	障害（法2条3項、政令2条1号）	例）療育手帳を交付され所持している	data concerning health
	身体障害、知的障害、精神障害（発達障害を含む。）その他の規則で定める心身の機能の障害*があること		
	病歴（法2条3項）	例）ガンにり患	
	診療等（法2条3項、政令2条3号）	例）インフルエンザのため、2月11日にA病院内科を受診した	
	健康診断等の結果に基づき、又は疾病、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又は診療若しくは調剤が行われ		
	健康診断等の結果（法2条3項、政令2条2号）	例）健康診断の結果、ストレスチェックの結果、特定健康診査の結果	
	本人に対して医師その他医療に関連する職務に従事する者（「医師等」）により行われた疾病の予防及び早期発見のための健康診断その他の検査（「健康診断等」）の結果		
犯罪等	犯罪の経歴（法2条3項）	例）強盗の前科2犯	
	刑事事件（法2条3項、政令2条4号）	例）窃盗を被疑事実として逮捕された	
	本人を被疑者又は被告人として、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		
	少年事件（法2条3項、政令2条5号）	例）少年時代に傷害で審判を受けた	
	本人を少年法3条1項に規定する少年又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		
犯罪被害	犯罪により害を被った事実（法2条3項）	例）空き巣に入られた	
機微情報（金融分野における個人情報保護に関するガイドライン）は、上記要配慮個人情報に以下が追加*1			
門地、本籍地		例）本籍地東京都千代田区〇〇	
労働組合への加盟		例）自治労に加入	trade union membership

性生活		例）アセクシャルである	data concerning a natural person's sex life or sexual orientation
保健医療		例）自己判断で市販薬を購入	
※日本法では要配慮個人情報ではなく、個人識別符号			genetic data, biometric data for the purpose of uniquely identifying a natural person

*1　本人、国の機関、地方公共団体、法第76条第１項各号若しくは施行規則第６条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。

顔認証・顔画像の比較

日本の個人情報保護法		GDPR	
個人識別符号：	△ 電子計算機で認証できるような顔認証、顔画像は「個人識別符号」に当たり、それ単体で、氏名等がわからなくても「個人情報」に当たる。多くの場合「個人データ」にも当たる。	Personal Data：	○
個人情報：	○ 電子計算機で認証できるような顔認証、顔画像は上記の通り「個人情報」「個人データ」に当たる。認証できないような顔画像は「個人識別符号」に当たらないものの、通常、それ単体で、氏名等がわからなくても誰の情報かわかると考えられ、「個人情報」に当たる。		
個人データ：	△ 電子計算機で認証できるような顔認証、顔画像は上記の通り「個人情報」「個人データ」に当たる。認証できないような顔画像は上記の通り「個人情報」に当たると考えられるが、「個人データ」に当たるかどうかはそれが検索できるよう体系的に構成されているか等、データの状態に依る。		
要配慮個人情報・機微情報：	× もっとも、履歴書に顔写真が貼られ、賞罰欄に前科が書かれていたりすると、前科は要配慮個人情報に当たるので、この履歴書は一体として要配慮個人情報に当たる。とはいえ、要配慮個人情報には当たるものの、要配慮になってもオプトアウトができないだけであるので、前科が書かれた履歴書が仮に送られてきたとしても、本人が任意で書いて提出したものであれば、本人同意があると考えられ、取得することはできる。	Special Categories of Personal Data：	△ 認証できるようなものだけ当たり、それ以外のものは当たらない。 ∵写真の取扱いは、特別な種類の個人データの取扱いであると即断してはならないとされている（前文51）。なぜなら、自然人を一意に識別又は認証をすることができる特別な技術的手段を用いて取扱われる場合においてのみ生体データに含まれるからである（前文51）