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