大手通信事業者における個人データの委託先の監督等について

〇昨今、電気通信事業者において、委託先を通じて大量の個人データの漏えいが発生する事案が複数発生しております。

〇個人データの取扱いを委託する場合には、委託先の選定、委託契約の締結及び委託先における個人データ等の取扱状況の把握等、委託先に対する必要かつ適切な監督を行う必要がありますが、昨今の事案においては、

・個人データの取扱いの委託が行われているにもかかわらず、委託先と再委託先の間の契約が業務委託契約ではなく、外部サービス利用契約であったことから、再委託の事実の把握や再委託先における個人データの取扱状況の把握が十分に行われていなかったケース

・個人データの委託先（再委託先を含む。）において、外部のクラウドストレージへのアクセスや外部記録媒体の利用が可能となっており、それらを通じて個人データが不正に持ち出されるなど、物理的安全管理措置、技術的安全管理措置等が不十分となっていたケース

など、委託先の監督が不十分であることに起因して、個人データの漏えいが発生しているケースが見受けられました。

〇特に、外部サービス利用契約については、同様の契約形態に伴う個人データの取扱いの委託が他の事業者においても行われていることが想定されるところ、個人データの取扱いを伴う外部サービス利用契約に係る認識や個人データの漏えい対策等を確認するため、今般、大手通信事業者における状況についてヒアリングを行うこととしました。

〇つきましては、以下の各項目について、委託先の監督に関する貴社の取組・状況をご記載ください。

社名		ＫＤＤＩ株式会社
１．委託先について		
1-1.	個人データの取扱いの委託（再委託）について、どのような情報を、どのような事業者に委託して	個人データの取扱いの委託先で取り扱う情報・事業者の代表例は以下のとおりです。

	いるのか、代表的なものを可能な範囲で記載すること。	■情報 ・サービスのお客様情報 ■事業者 ・携帯販売代理店（契約取次業務の委託業務） ・コールセンター（お客様対応業務の委託業務）
1-2.	個人データの委託（再委託）について、委託先との間の契約形態にはどのような種別があるか（業務委託、定型のサービス利用規約に基づくもの等）。	委託先との契約形態の種別は以下のとおりです。 ・業務委託 ・定型のサービス利用規約に基づくもの
２．委託先の監督について　※1-2 の契約種別毎に異なる場合は、種別毎に一般的な内容を記載すること（様式別途でも可）。		
（１）外部サービス利用に対する認識		
2-1	個人データを取り扱う情報システムに外部サービスを活用する場合において、当該外部サービスの提供者が当該個人データを取り扱う場合、個人情報保護法上の委託に該当するものとして扱っているか。	個人データを取り扱う外部サービスの提供形態によりますが、個別の事案ごとに法令に則った対応を行っています。
2-2	2-1 の回答が「個人データの委託として扱っている」の場合、個人データの取扱いの委託先における安全管理措置の実施、秘密保持、	個人データについて委託として取り扱っている場合は社間で、主に以下内容を義務として委託先に課す契約を締結しております。 ・利用目的の限定 ・秘密保持

	再委託の条件、再委託先の監督等について、契約上どのように担保されているか（外部サービス利用契約又はそれに付随する覚書等における標準的な記載の例を示すこと）。	・従業員の監督 ・再委託の制限 ・管理状況の報告・調査 ・預託した情報の返還、消去等 ・損害賠償
2-3	個人データの取扱いの委託先が、当該個人データを取り扱う情報システムに外部サービスを活用する場合において、当該外部サービスの提供者が当該個人データを取り扱う場合、個人情報保護法上の再委託に該当するものとして扱っているか。	個人データを取り扱う外部サービスの提供形態によりますが、個別の事案ごとに法令に則った対応を行っています。
2-4	2-3 の回答が「個人データの再委託として扱っている」の場合、個人データの取扱いの委託先による再委託先の監督や、貴社による再委託先の監督について、契約上どのように担保されているか（外部サービス利用契約又はそれに付随する覚書等における標準的な記載の例を示すこと）。	個人データについて再委託として取り扱っている場合は、2-2 回答の契約において、委託先に課している内容と同等の義務を、委託先が再委託先に対して課すこととしています。
（２）委託先の選定		

2-5	個人データの取扱いを委託する場合において、委託先（再委託先を含む）の選定にあたり、個人データを適切に取り扱うための安全管理措置が講じられているかについて確認を行っているか。確認を行っている場合、具体的にどのような項目を、どのような方法で確認しているか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	委託先の選定にあたり、以下の安全管理措置の確認を行っています。 （以下、構成員限り） [redacted]
2-6	個人データの取扱いの委託先の選定にあたり、委託先（再委託先を含む）における教育体制（教育対象の社員の範囲、研修の有無、理解度の確認、研修内容の見直し、頻度等）について、どのようなものを求めているか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	委託先の選定にあたり、以下のとおり教育体制の整備を求めています。 （以下、構成員限り） [redacted]
（３）委託契約の締結		
2-7-1	個人データの取扱いに係る委託契約（再委託契約を含む）において、安全管理措置の実施、秘密保持、再委託の条件、再委託先の監	委託契約内で安全管理措置の実施、秘密保持、再委託の条件、再委託先の監督に関する事項を以下のとおり定めています。 （以下、構成員限り） [redacted]

	督等に関する事項を定めているか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	[redacted]
2-7-2	自社の個人データの取扱いを委託している場合において、1-7-1 のとおり委託契約（再委託契約を含む）に定めた事項について、契約書締結以外の方法により実運用上行っている措置はあるか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	契約書締結以外の方法により行っている実運用上の措置は、以下のとおりです。 （以下、構成員限り） [redacted]
2-8	個人データの取扱いの委託先が再委託を行う場合、委託先に対してどのような対応を行っているか（再委託を承諾する基準等の再委託条件、委託先による再委託先の管理監督の実施状況の把握方法等）。	再委託を行う場合も、委託先から再委託先に対し、2-7-1 と同じ条件を求めています。その他委託先に対し求めている事項は、以下のとおりです。 （以下、構成員限り） [redacted]

	※1-2 の種別で差異がある場合には、それぞれ記載すること。	
（４）個人データの取扱いの委託先における個人データの取扱状況の把握		
2-9	個人データの取扱いの委託先（再委託先を含む）における個人データの取扱状況について、どのように把握し、監督を行っているか。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	委託先における個人データの取扱い状況について、以下のとおり把握、監督をしています。 （以下、構成員限り） [redacted]
2-10	個人データの取扱いの委託先（再委託先を含む）における個人データの取扱いの監査・点検の内容、方法及び頻度並びに 2023 年度の実施件数（書面点検・立ち入り調査の各件数）。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	委託先における個人データの取扱いの監査・点検の内容、方法、頻度、実施件数は以下のとおりです。 （以下、構成員限り） [redacted]

（５）個人データの取扱いの委託及び再委託の実施状況		
2-11	電気通信事業に係る個人データの取扱いの委託先及び再委託先の件数。 （内数として以下を記載） ・外部サービスの利用 ・親会社、連結子会社に係るもの	電気通信事業に係る個人データの取扱いの委託先及び再委託先の件数は以下のとおりです。 （以下、構成員限り） [redacted]
2-12	個人データの取扱いの委託先（再委託先を含む）における、個人データの取扱いに係る契約違反の件数（2023 年度）。 ※1-2 の種別で差異がある場合には、それぞれ記載すること。	2023 年度における委託先・再委託先における個人データの取扱いに係る契約違反は以下のとおりです。 （以下、構成員限り） [redacted]
３．その他		
（１）物理的・技術的安全管理措置		
3-1	外部からの不正アクセスによる個人データの漏えいを防ぐため、どのような安全管理措置を講じてい	業務委託先における外部からの不正アクセス及び内部からの不正な持出しによる安全管理措置として、以下の措置を実施しています。

	るか。特に、個人データにアクセスする場合の従業員の認証等、技術的安全管理措置をどのように講じているか。	（以下、構成員限り） [redacted]
3-2	内部からの不正な持ち出しによる個人データの漏えいを防ぐため、どのような安全管理措置を講じているか。特に、実際に不正な持ち出しを行おうとした場合に、それを阻止するための物理的・技術的安全管理措置をどのように講じているか 少なくとも以下の内容については、具体的に対応状況の回答をお願いします。 -許可されていない外部ストレージへのアクセスが可能となっていないか - 保守作業端末にダウンロードが可能になっていないか - 保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていないか - セキュリティリスクが大きいと想定される振る舞いを即時に検知できているか	

	－各種ログ等の定期的なチェックは十分か	
（２）委託に関する利用者への説明		
3-3	個人データの取扱いを外部へ委託することについて、利用者に対してどのような説明を行っているか。	個人データの取扱いを外部へ委託することがある旨の説明は、KDDI プライバシーポリシー上で説明しています。 ※参考 https://www.kddi.com/corporate/kddi/public/privacy/ https://www.kddi.com/corporate/kddi/public/privacy/annex7/#7-2
（３）漏えい発生後の対応		
3-4	漏えいの発生後の対応として、漏えいした情報がインターネット上に流通していないかを検知したり、作業者の記録を保存し漏えいの発生原因を特定したりすることができるよう、措置を行っているか。	漏えい情報の検知及び発生原因の特定については、以下のとおりの措置を行っています。 （以下、構成員限り） [redacted]