2018年1月15日（月）監査女子会ディナー・ミーティング　配布資料（取扱注意）
GDPRはやわかりダッシュ解説（細かくは色々あるけど戸村版で速習）

◆GDPRの「R」が意味すること：　指令ではなく規則⇒EU全域で共通の決まりを共通に適用・運用する
◆日本の改正個人情報保護法との大きな違いを一言で言うと・・・
GDPR＝「入口が狭い」（プライバシー・人権重視）、日本＝「出口が狭い」（漏えい対策重視）

◆GDPRのはやわかりっていっても、「でも、お高いんでしょ～？」⇒ はい、めちゃくちゃ高いです！
課徴金（比較的軽微な問題）：　1,000万ユーロor全世界年間売上高の2%上限
課徴金（域外移転・比較的重い問題）：　2,000万ユーロor全世界年間売上高の2%上限
⇒課徴金の低減要素(GDPR第83条2っぽくみると・・・)で改正個人情報保護法の安全管理措置も該当

【主なポイントを6つに絞って下記にまとめてみると・・・】

① **企業等への効力＆域外適用**：　2018年5月25日より。EUに拠点（支社・支店でなくとも連絡所などでも）があれば当然に域内で適用。域外適用として、EU向けに商品・サービス・ウェブ決済などを行っている場合や、支払い通貨にユーロが選べるサービスなどは、域外適用の可能性が高くなる。（EU内の消費者が購入・利用可能な状態かどうかが分かれ目になりやすい）
The offering of goods or servicesかEU域内データ主体の行動監視の有無で域外適用か否か決定
⇒日本法人がEU域内の従業員情報を扱う場合、域外適用でなく**域外移転**（EU→日本）だけ問題
（ITシステム関連でもデータ処理に困ったら…：「2001/497/EC」標準契約条項を調べておく）

② **データ収集時の12項目の情報提供義務**（入口が狭い：人権・プライバシー意識の高いEUっぽい）
・データ管理者の身元と連絡先等　・データ保護責任者(いる時)の連絡先等　・処理目的と法的根拠
・管理者or第三者にに求められる正当なメリット　・個人データ取得者または取得者の種類(ある場合)
・第三国や国際的にデータ移転する意図がある場合はその意図とデータ保護の十分性や安全保護に関する措置等とその証跡コピー入手方法　・データ保存期間等　・訂正や削除権等について
・同意がいつでも撤回可能なことと撤回前の処理は合法であり続ける旨の記載　・監督機関に不服申し立てできる権利について　・個人データの提供が法的/契約的に必要要件であるかどうかやデータ提供の不履行で起こり得る結果やデメリット等　・データによるプロファイリングを含めた自動化された意思決定処理の有無等　といった12項目が名刺受けなどにすら明記・掲出されている必要あり

③ **GDPRの「個人データ」＝EU域内に所在する個人の情報**
EU域内に居住しているかどうかは関係ない（EU域内に赴任した日本人の役職員の個人データも、GDPRの「個人データ」に該当）

④ **沈黙の同意（黙示的な同意）は同意として機能しない＆雇用主の優越的地位の勘案**
「チェックボックスのチェックを外さなかった場合は、個人情報を提供することに同意したとみなします」という対応は違法となる
雇用主は強い立場にあるとされ、弱い立場にいる労働者のデータ処理に関しては、個人データ主体の情報取扱いの判断などにおける権利保護で、より慎重に対応しなければならない（ハイリスク評価）

⑤ **個人データ管理者の義務**
個人データの漏えい・権利侵害が生じた際は、可能な限りは侵害を認識してから72時間以内に監督機関に通知しなければならない（33条1）（管理者下の処理者は侵害を認識してから不当に遅滞なく管理者に通知しなければならない）

⑥ **GDPRでの域外へのデータ移転**は、①基本的には対象国の十分性をクリアしていることがベストだが、代替的には、②標準契約条項などによる安全措置によって移転するのがベターである一方で、どうしても仕方ない場合は、③データ主体の同意を得て域外移転する。

←監査女子会のページ

資料作成：　JMRI, LLC.　戸村智憲
https://www.jmri.co.jp/