ECDL / ICDL Data Protection (Ochrana osobních údajů)
SYLABUS 1.0 (M21)

The Digital Skills Standard

Modul M?? Ochrana osobních údajů

Sylabus ECDL / ICDL Data Protection (Ochrana osobních údajů) vymezuje rozsah znalostí a dovedností, které jsou nezbytné k pochopení základních pojmů a smyslu ochrany osobních údajů, a které jsou nutné pro úspěšné složení mezinárodní ECDL zkoušky z tohoto modulu.

Cíle modulu

Modul M21 Úspěšný absolvent zkoušky z tohoto modulu by měl …

- Rozumět hlavním zásadám ochrany osobních údajů.
- Rozumět důvodům, cílům a rozsahu obecného nařízení Evropské unie o ochraně osobních údajů (General Data Protection Regulation - GDPR).
- Znát klíčové zásady GDPR ve vztahu k zákonnému zpracování osobních údajů.
- Vědět, že subjekty údajů mají svá práva a znát způsoby, jak mohou být uplatňována.
- Vědět, že pravidla v organizaci by měla být v souladu s nařízením GDPR a umět popsat klíčové technické a organizační opatření potřebná k naplnění smyslu tohoto nařízení.
- Vědět, jak postupovat v případě narušení bezpečnosti osobních údajů a jak vyřešit důsledky porušení GDPR.

KATEGORIE	OBLAST ZNALOSTÍ		ODKAZ	ROZSAH ZNALOSTI
21.1 Základní pojmy	21.1.1	Osobní údaje	21.1.1.1	Rozumět pojmu soukromí a s ním spojených práv. Uvědomovat si, že soukromí není absolutním právem a jiná práva mohou být nadřazená.
			21.1.1.2	Rozumět pojmu osobní údaje.
			21.1.1.3	Rozumět pojmu zpracování osobních údajů.
			21.1.1.4	Uvědomovat si rozdíl mezi automatizovaným a ručním zpracováním osobních údajů.
	21.1.2	Ochrana osobních údajů	21.1.2.1	Rozumět pojmu ochrana osobních údajů.
			21.1.2.2	Znát rizika, která mohou hrozit osobním údajům jako jsou náhodné nebo nezákonné zničení, ztráta, nepravdivé pozměňování, nezákonné zveřejnění nebo nezákonný přístup.
			21.1.2.3	Znát rizika, která mohu hrozit subjektům údajů při zpracování jejich osobních údajů jako jsou diskriminace, krádež či zneužití totožnosti, poškození dobrého jména, ztráta důvěryhodnosti, ztráta soukromí, omezení práv, ztráta kontroly na osobními údaji nebo profilování a jejich ekonomické důsledky.
			21.1.2.4	Znát role a odpovědnosti zúčastněných stran jako jsou subjekt údajů, zpracovatel osobních údajů, správce osobních údajů a pověřenec pro ochranu osobních údajů.
21.2 GDPR	21.2.1	Důvody a cíle	21.2.1.1	Vědět, že GDPR je obecné nařízení Evropské unie, které je právně vymahatelné na území všech členských států.
			21.2.1.2	Chápat důvody pro zavedení nařízení GDPR jako jsou zvýšení právní jistoty, zvýšení jistoty a důvěry spotřebitelů, rostoucí objem zpracovávaných osobních údajů a jejich sdílení mezi zeměmi.
			21.2.1.3	Umět popsat hlavní cíle nařízení GDPR jako jsou zajištění patřičné úrovně ochrany osobních údajů fyzických osob, zajištění bezpečného sdílení osobních údajů v rámci zemí Evropské unie.
	21.2.2	Rozsah	21.2.2.1	Uvědomovat si rozsah činností v oblasti zpracování osobních údajů, který pokrývá nařízení GDPR jako je automatizované a manuální zpracování osobních údajů, a znát činnosti spojené se zpracováním osobních údajů, které nepodléhají tomuto nařízení.
			21.2.2.2	Uvědomovat si územní působnost nařízení GDPR ve vztahu k místu zpracování osobních údajů a místní příslušnosti subjektu údajů.
21.3 Hlavní zásady	21.3.1	Zpracování osobních údajů	21.3.1.1	Rozumět zásadám zákonnosti, spravedlnosti a transparentnosti.
			21.3.1.2	Rozumět zásadě omezení účelu zpracování osobních údajů.
			21.3.1.3	Rozumět zásadě minimalizace rozsahu zpracovávaných osobních údajů.
			21.3.1.4	Rozumět zásadě správnosti osobních údajů.

KATEGORIE	OBLAST ZNALOSTÍ		ODKAZ	ROZSAH ZNALOSTI
			21.3.1.5	Rozumět zásadě omezení ukládání osobních údajů.
			21.3.1.6	Rozumět zásadám integrity a důvěrnosti osobních údajů.
			21.3.1.7	Rozumět zásadě odpovědnosti při zpracování osobních údajů.
	21.3.2	Zákonné zpracování osobních údajů	21.3.2.1	Znát zákonné důvody pro zpracování osobních údajů jako jsou souhlas subjektu údajů, zpracování osobních údajů na základě smlouvy, plnění zákonných povinností správce, ochrana oprávněných zájmů zpracovatele nebo zpracování osobních údajů ve veřejném zájmu.
			21.3.2.2	Uvědomovat si, že souhlas se zpracováním osobních údajů může být platný jen za splnění určitých podmínek. Znát podmínky pro udělení souhlasu jako jsou prokazatelnost udělení souhlasu, jasná specifikace osobních údajů, odvolatelnost souhlasu nebo svobodná vůle.
			21.3.2.3	Znát pravidla pro udělení souhlasu se zpracováním osobních údajů nezletilých osob při registraci u internetových služeb.
			21.3.2.4	Vědět, že v případě zpracování údajů jménem správce osobních údajů, musí existovat smluvní vztah mezi správcem a zpracovatelem, který zajistí soulad s nařízením GDPR a který bude garantovat dodržování zásad zpracování osobních údajů.
			21.3.2.5	Znát zvláštní kategorie osobních údajů, jejichž zpracování je možné pouze při existenci zvláštních právních důvodů jako jsou rasová či etnická příslušnost, politické názory, náboženská vyznání nebo filozofická přesvědčení, členství v odborových organizacích, informace o zdravotním stavu nebo sexuální orientace.
			21.3.2.6	Vědět, že osobní údaje mohou být předávány ke zpracování mimo země Evropské unie pouze tehdy, když externí směrnice ochrany osobních údajů jsou v souladu s nařízením GDPR.
21.4 Práva subjektu údajů	21.4.1	Uplatnění práv	21.4.1.1	Uvědomovat si důležitost transparentní komunikace se subjektem údajů při zpracování osobních údajů jako jsou upozornění na ochranu soukromí nebo zveřejnění zásad ochrany osobních údajů.
			21.4.1.2	Znát klíčové informace, které musí být poskytnuty subjektu údajů při získávání osobních údajů jako jsou identifikace správce a zpracovatele osobních údajů včetně jejich kontaktních údajů, účel zákonného zpracování osobních údajů, doba uchování osobních údajů nebo seznam práv subjektu údajů.
			21.4.1.3	Vědět, že mohou existovat doplňující informace, které by měly být poskytnuty subjektu údajů při získávání osobních údajů správcem jako jsou přenos osobních údajů do třetí země, kontaktní informace na pověřence pro ochranu osobních údajů nebo další zpracovatelé osobních údajů.
			21.4.1.4	Uvědomovat si, že doplňující informace by měly být poskytnuty subjektu údajů i v případě, kdy osobní údaje nejsou získávány přímo správcem osobních údajů.
	21.4.2	Práva subjektu údajů	21.4.2.1	Rozumět pojmu žádost o přístup subjektu údajů a rozumět právu subjektu údajů na přístup ke svým zpracovávaným osobním údajům.
			21.4.2.2	Rozumět právu na opravu, resp. doplnění osobních údajů.
			21.4.2.3	Rozumět právu na výmaz (být zapomenut).
			21.4.2.4	Rozumět právu na omezení zpracování.
			21.4.2.5	Rozumět právu na přenositelnost údajů.
			21.4.2.6	Rozumět právu nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnujíce i profilování.
			21.4.2.7	Chápat, že práva subjektu údajů nemusí být vždy dodržena, pokud existují zákonná omezení.
21.5 Zavádění	21.5.1	Pravidla a metody	21.5.1.1	Chápat, že směrnice a pravidla pro zpracování osobních údajů musí být v souladu s nařízením GDPR. Uvědomovat si nutnosti tato pravidla a směrnice dodržovat.

KATEGORIE	OBLAST ZNALOSTÍ		ODKAZ	ROZSAH ZNALOSTI
			21.5.1.2	Uvědomovat si, že zpracování osobních údajů by mělo automaticky vycházet ze stanovených pravidel.
			21.5.1.3	Rozumět pojmu posouzení dopadu na ochranu osobních údajů a vědět, kdy je vyžadováno.
	21.5.2	Opatření	21.5.2.1	Rozpoznat vhodná technická a organizační opatření pro řízení rizik při zpracování osobních údajů jako jsou pseudonymizace osobních údajů a šifrování dat, zajištění trvalé důvěrnosti a integrity dat, zajištění dostupnosti a odolnosti systémů a služeb nebo schopnosti obnovit osobní údaje.
			21.5.2.2	Znát specifická technická opatření pro řízení rizik při zpracování osobních údajů jako jsou šifrování dat, bezpečné digitální úložiště, zálohování dat, bezpečný způsob digitální komunikace, bezpečné fyzické prostředí nebo bezpečná likvidace dat.
			21.5.2.3	Znát specifická organizační opatření pro řízení rizik při zpracování osobních údajů jako jsou školení, procesy a postupy, smluvní vztahy, manažerský dohled.
			21.5.2.4	Chápat rozdíl mezi pseudonymizací a anonymizací osobních údajů.
21.6 Soulad s GDPR	21.6.1	Narušení bezpečnosti	21.6.1.1	Rozumět pojmu narušení bezpečnosti osobních údajů.
			21.6.1.2	Vědět, za jakých okolností musí správce osobních údajů oznámit narušení bezpečnosti osobních údajů kontrolnímu orgánu. Uvědomovat si, že existuje časová lhůta pro toto oznámení.
			21.6.1.3	Uvědomovat si, že správce osobních údajů by měl oznámit narušení bezpečnosti osobních údajů subjektu údajů když existuje vysoké riziko porušení práv subjektů údajů.
	21.6.2	Vymáhání	21.6.2.1	Vědět, která státní organizace je dozorovým orgánem v oblasti ochrany osobních údajů a znát své zákonné povinnosti vůči tomuto orgánu.
			21.6.2.2	Vědět, že subjekt údajů má právo k podání stížnosti k dozorovému orgánu bez ohledu na to, kde jsou jeho osobní údaje zpracovávány.
			21.6.2.3	Uvědomovat si možné důsledky nedodržování zákonem stanovených opatření na ochranu osobních údajů jako jsou pokuty, soudní spory nebo poškození dobrého jména.