

**Zmluvné výskumné
služby**

**WP2 Počítačová bezpečnosť a ochrana a
súkromie osobných údajov**

D2.2 Ochrana osobných údajov

AtoS

Pracovný balík	WP2 Počítačová bezpečnosť a ochrana a súkromie osobných údajov			
Úloha	T2.2			
Dátum dodania	Zmluvný	Október 2015	Skutočný	Október 2015
Názov kódu	WP2 - D2.2 Ochrana osobných údajov		Verzia 1.0 Návrh	
Typ dodávky	Správa			
Autori	Nicolás Notario			
Krátky abstrakt	Štúdia aktuálneho stavu súkromia v oblasti projektovania (PbD), odporúčania pre organizácie a pre všetky metodológie PbD, ktorých cieľom je vytvoriť systémy ICT dodržiujúce súkromie.			
Projektový manažér zákazníka	Jozef Vodny (Atos Slovakia) Tel: +421268526684; Mobile: +421903573148 email: jozef.vodny@atos.net			
Projektový manažér poskytovateľa	Alicia Garcia (Atos Spain) Tel: +34 91214 8800; Mobile: +34 625 598 562 email: alicia.garcia@atos.net			

1	Skratky	6
2	Výkonné zhrnutie	8
3	Úvod.....	9
3.1	Ciele dodávky	9
3.2	Štruktúra dokumentu.....	9
4	Spoločné PbD a koncepty ochrany údajov	12
5	Analýza a hodnotenie existujúcich prístupov PbD	16
5.1	Princípy súkromia	16
5.2	Hodnotenia vplyvu na súkromie (PIA)	16
5.3	Organizácia pre napredovanie noriem štruktúrovaných informácií (OASIS)	18
5.3.1	PMRM	18
5.3.2	PBD-SE.....	21
5.4	Metodológie hodnotenia rizík súkromia.....	24
5.4.1	Metodológia rizika súkromia CNIL.....	25
5.4.2	LINDDUN	28
5.4.3	Návrh riadenia rizika súkromia NIST	29
5.4.4	BSI PIA.....	30
5.5	Súkromie zamerané na cieľ	31
5.6	Bezpečnosť.....	32
5.6.1	Cyklus životnosti rozvoja bezpečnosti u Microsoftu	32
5.6.2	Otvorený projekt bezpečnosti webových aplikácií (OWASP)	33
5.6.3	Ostatné veľké bezpečnostné iniciatívy	34
5.7	Normy súkromia a orgány	35
5.8	Súkromie softvéru verus hardvéru	36
5.9	Technológie podpory súkromia softvéru	36
5.9.1	Technológie podpory transparentnosti (TET)	36
5.9.2	Nástroje preferencie súkromia	38
5.10	Technológie podpory súkromia hardvéru	38
5.10.1	Riadenie prístupu k identite	38
5.10.2	Úroveň komunikácie	39
5.10.3	Úroveň ukladania	40
5.10.4	Úroveň počítania	42
5.11	Architektonické prístupy	43
5.11.1	Architektúry podporujúce súkromie	43
5.11.2	Vzorce súkromia	43

5.11.3	Stratégie projektu súkromia	44
5.12	Holistický prístup.....	44
6	Odporúčaná metodológia PbD pri riadení projektu systému bezpečnosti ICT	46
7	Preukázanie výhod PbD	54
7.1	Smart Grid	54
7.2	Internet of Things	54
7.3	LINDDUN	55
7.4	PRIPARE.....	55
8	Referencie	56

Zoznam tabuliek

Tabuľka 1: Prevádzkové služby PMRM [28]	21
Tabuľka 2: Príklady dokumentácie a vizuálne modely súkromia	24
Tabuľka 3: Vzorec závažnosti CNIL	27
Tabuľka 4: Príklad výpočtu závažnosti CNIL	27
Tabuľka 5: Vzorec odhadu pravdepodobnosti CNIL.....	27
Tabuľka 6: Príklad výpočtu pravdepodobnosti CNIL	27
Tabuľka 7: Návrh CNIL na mapu rizika	28
Tabuľka 8: Fázy a postupy SDL Microsoftu	33

Zoznam obrázkov

Obrázok1: Konceptný model PMRM [HYPERLINK \I "PMRM" 28]	19
Obrázok 2: Prehľad metodológie PMRM [28]	19
Obrázok 3: Fázy riadenia rizika.....	25
Obrázok 4: Fázy a ciele riadenia rizika	25
Obrázok 5: Model stanovenia miery rizika CNIL	26
Obrázok 6: 6 krokov LINDDUN	29
Obrázok 7: Rámec riadenia rizika súkromia NIST (PRMF)	30
Obrázok 8: Rozklad vplyvu BSI	31
Obrázok 9: Kroky metodológie hodnotenia rizík OWASP	34
Obrázok 10: Proces navrhovaný PRIPARE [38].....	50

1 Skratky

ASVS	Norma overovania bezpečnosti aplikácií
BSI	Bundesamt für Sicherheit in der Informationstechnik
CNIL	Národná komisia pre informatiku a slobodu
COBIT	Kontrolné ciele pre informačné a príslušné technológie
DFD	Diagram toku údajov
DPA	Autorita ochrany údajov
EBIOS	Vyjadrenie potrieb a identifikácia bezpečnostných cieľov
EC	Európska komisia
ENISA	Agentúra Európskej únie pre bezpečnosť sietí a informačnú bezpečnosť
FIPPs	Férové informačné postupy a princípy
ICO	Kancelária informačného komisára
ICT	Informačná komunikačná technológia
IoT	Internet prvkov
IoT-A	Internet prvkov – Architektúra
IPR	Práva duševného vlastníctva
IPSec	Bezpečnosť internetového protokolu
ISO	Medzinárodná organizácia pre normy
JFK	Just Fast Keying
LINDDUN	Spojovateľnosť, Identifikovateľnosť, Uznávanie, Detekovateľnosť, Šírenie informácií, Nepoznanie, Nezhoda
LUKS	Jednotné nastavenie kľúčov Linux
MAC	Kontrola prístupu k médiám
MPC	Postupy výpočtov viacerých strán
NIST	Národný inštitút pre normy a technológiu
OASIS	Organizácia pre pokrok v oblasti štruktúrovaných informačných noriem
OECD	Organizácia pre hospodársku spoluprácu a rozvoj
OWASP	Otvorený projekt bezpečnosti webových aplikácií
P3P	Platforma pre preferencie súkromia
PbD	Súkromie na základe projektu
PbD-SE	Súkromie projektovej dokumentácie pre softvérových inžinierov
PEAR	Architektúra podporujúca súkromie
PET	Technológia podporujúca súkromie
PGP	Dosť dobré súkromie
PI	Osobné informácie
PIA	Hodnotenie vplyvu súkromia
PIAF	Rámce hodnotenia vplyvu na súkromie
PII	Osobné identifikačné informácie
PMRM	Referenčný model riadenia súkromia
PRIPARE	Príprava odvetvia na súkromie projektu podporou výskumu aplikácií
PRMF	Rámec riadenia rizika súkromia
RFID	Identifikácia rádiových frekvencií
SAMM	Model zrelosti zaistenia softvéru
SDL	Životný cyklus rozvoja bezpečnosti
SSH	Bezpečný rámec
STRIDE	Krádež identity, Narušenie údajov, Neuznanie, Šírenie informácií, Odmietnutie služby, Zvýšenie privilégia
TET	Technológie podporujúce transparentnosť
TLS	Bezpečnosť prepravnej vrstvy
TOR	The Onion Routing
UI	Používateľské rozhranie
UML	Jednotný modelovací jazyk

VoIP	Voice over IP
VPN	Virtuálna súkromná sieť
W3C	Webové konzorcium
WAI	Smernice webovej dostupnosti
WCAG	Smernice dostupnosti webového obsahu

2 Výkonné zhrnutie

Riešenie súkromia v metodológii, kde sa musia zhodnúť rôzni účastníci (napr. inžinieri, právnici, dátové subjekty, poskytovatelia služieb) si vyžaduje stanovenie spoločného jazyka už od začiatku. PbD, riadenie rizík, koncepty súkromia a ochrany údajov ako je **zodpovednosť** alebo **súhlas** sa získajú a uvedú v glosári pomocou autoritatívnych zdrojov ako sú ISO alebo CNIL.

Princípy súkromia na vysokej úrovni sa od svojho prvého vývoja výrazne nezmenili. Avšak na základe toho, že sa veľmi ťažko ovládajú v systémoch ICT, vyvinuli sa mnohé prístupy, aby sa tieto princípy súkromia zmenili na prenikajúci majetok obchodných procesov a systémov. Príslušné prístupy sú prepojené a snažia sa doplniť a riešiť medzery zistené predtým. Hodnotia sa nasledujúce prístupy:

- Hodnotenie vplyvu na súkromie;
- Prístupy OASIS (PMRM a PbD-SE);
- Hodnotenia rizika súkromia;
- Súkromie zamerané na cieľ;
- Normy v oblasti súkromia;
- Softvérové a hardvérové technológie podporujúce súkromie;
- Riešenie súkromia na architektonickej úrovni;
- Holistické súkromie.

Na záver tejto aktuálnej štúdie sa vydali odporúčania pre každú organizáciu a metodológiu PbD, ktorých cieľom je vytvoriť systémy ICT dodržiavajúce súkromie:

- Vybudovať štruktúru súkromia na organizačnej úrovni;
- Zapojiť všetkých účastníkov počas inžinierskych procesov;
- Transparentnosť;
- Zameranie na používateľa;
- Súkromie musí pokrývať celé budovanie a cyklus životnosti osobných údajov;
 - Popis na vysokej úrovni a úvodné hodnotenie;
 - Príprava plánu súkromia;
 - Požiadavky súkromia;
 - Projekt súkromia;
 - Implementácia a overenie súkromia;
 - Kontroly súkromia systému pred prevádzkou;
 - Prevádzka systému a vyradenie s podporou súkromia.

Nie je jednoduché preukázať výhody aplikácie prístupov technológie PbD. Niektoré prípady úspechu, spojené s IoT a smart grid domains sú však nasledujúce:

- Hodnotenie vplyvu súkromia, ktoré sa vykonalo v mene asociácií energetických sietí;
- Súkromný protokol plnenia elektrického vozidla, dodržiavajúci všetky funkcie ISO15118;
- Referenčný model architektúry dodržiavajúci súkromie pre vzájomnú prevádzkyschopnosť systémov Internet-of-Things.

3 Úvod

3.1 Ciele dodávky¹

Cieľom tejto dodávky je vypracovať konečnú vedeckú správu, ktorá analyzuje spoločné koncepty a prístupy v dnešnej praxi PbD pre vytvorenie hlavnej metodológie PbD, ktorá sa použije v projekte a rozvoji bezpečných systémov ICT. V rámci toho bude táto správa identifikovať a zohľadňovať medzery v aktuálnych prístupoch, ktoré fungujú ako bariéry pre kompletné zvládnutie PbD v systémoch ICT. V tejto správe sa bude napokon uvádzať príklad používania odporúčaného prístupu PbD v kontexte bezpečnostných systémov ICT.

3.2 Štruktúra dokumentu

Tento dokument bude rozdelený do štyroch hlavných kapitol:

- SpoločnýSpoločné PbD a koncepty ochrany údajov: uvádza najbežnejšie a/alebo najviac relevantné koncepty súkromia, ktoré stanovujú základy pre hodnotenie prístupov PbD a/alebo postupov;
- Analýza a hodnotenie existujúcich prístupov PbD: naviguje z najjednoduchších prístupov súkromia (princípy súkromia) na najnovšie a holistické prístupy (PRIPARE), ktoré identifikujú jeho medzery spojenia s ostatnými postupmi. Analyzované prístupy súkromia boli zvolené po komplexnej revízii literatúry a na základe ich relevantnosti, komplementarity a pravouhlosti;

¹ Klient formálne súhlasil s tým, že popis ochrany osobných údajov si vyžadoval výstup uvedený v časti 2.2.2.2 prílohy 1 Dohoda o zmluvnom výskume zodpovedá časti T2.1 a následne je nepresná pri T2.2. Preto sa požadovaný výstup popísaný v časti 2.2.2.2 poskytne v časti D2.1, dodávka zodpovedá časti T2.1 Počítačová bezpečnosť. Výstup T2.2 Ochrana osobných údajov sa vzťahuje na popis časti T2.2 (pozrite si časť 2.2.2.1 dohody) a je popísaný vyššie v časti 3.1 Ciele dodávky.

4 Odporúčaná metodológia PbD pri riadení projektu systému bezpečnosti ICT

- : budovanie na základe predchádzajúcej analýzy a zohľadnenie identifikovaných medzier, poskytujú sa smernice pre organizácie, ktoré implementujú metodológie PbD;

5 Preukázanie výhod PbD

- : je tu uvedený výber prípadov úspešného využívania aplikácie postupov PbD, ktoré sú uvedené v hodnotení prístupov PbD

6 Spoločné PbD a koncepty ochrany údajov

Zodpovednosť

„Princíp určený na zaistenie toho, aby mali kontrolóri lepšiu celkovú kontrolu a aby boli v pozícii, aby mohli a preukázať zhodu s princípmi ochrany údajov v praxi. Zodpovednosť si vyžaduje, aby kontrolóri zaviedli interné mechanizmy a kontrolné systémy, ktoré zaisťujú zhodu a poskytujú dôkazy – ako sú správy o audite – aby preukázali zhodu s externými účastníkmi, vrátane kontrolných orgánov“ [[HYPERLINK \I "EDPSAccountability" 1](#)].

Anonymita

„Vlastnosť informácií, ktorá neumožňuje priamu ani nepriamu identifikáciu osobne identifikovateľných informácií“2].

Anonymizácia

„Proces, ktorým sa osobne identifikovateľné informácie (PII) nevratne zmenia takým spôsobom, že PII sa už nebude dať priamo alebo nepriamo identifikovať, buď pomocou samotného ovládača PII alebo v spolupráci s nejakou inou stranou“ [[HYPERLINK \I "ISO29100" 2](#)]. Avšak článok 29 potvrdzuje, že „prípadové štúdie a výskumné publikácie ukázali, aké je zložité vytvoriť skutočne anaonymnú sústavu údajov pri zachovaní čo najväčšieho objemu základných informácií požadovaných pre danú úlohu“3] a že „kontrolóri údajov by mali zvážiť to, že anonymizovaná sústava údajov môže predstavovať zvyškové riziká pre dátový subjekt“.

Súhlas alebo informovaný súhlas

„V terminológii ochrany údajov sa súhlas vzťahuje na špecifickú a informovanú indikáciu želaní dátového subjektu, ktorou súhlasí s osobnými údajmi, ktoré sa naňho vzťahujú a ktoré sa spracovávajú (pozrite si článok 2 odsek (h) smernice ochrany údajov 95/46/EC [[HYPERLINK \I "Eur951" 4](#)] a článok 2 odsek (h) nariadenia (EC) č. 45/20015].“ [[HYPERLINK \I "EDPSConsent" 6](#)] článok 29 Pracovná strana vydala odporúčanie7] s explicitnejšou požiadavkou, ktorá by mala skutočne dosiahnuť informovaný súhlas:

- „Ak má byť tento súhlas platný, musí byť špecifický a musí byť založený na vhodných informáciách. Inými slovami, prázdny súhlas bez špecifikácie presného účelu spracovania nie je prijateľný“
- „Vo všeobecnosti sa musí súhlas vydať pred začiatkom spracovania“
- „Súhlas musí byť jednoznačný. Preto postup hľadania a udelenia súhlasu nesmie zanechávať žiadne pochybnosti, pokiaľ ide o zámer dátového subjektu“
- „Súhlas môže byť platný len vtedy, ak dokáže dátový subjekt vykonať skutočný výber a neexistuje riziko podvodu, vydierania, donucovania alebo výrazných negatívnych následkov v prípade, že nesúhlasí“

Kontrolór údajov

„Fyzická alebo právnická osoba, verejný orgán, agentúra alebo iný orgán, ktorý sám alebo spoločne s ostatnými stanovuje ciele a prostriedky spracovávania osobných údajov; (článok 2 d)“ [[HYPERLINK \I "Eur951" 4](#)].

Minimalizácia údajov

„Princíp „minimalizácie údajov“ znamená, že kontrolór údajov by mal obmedziť získavanie osobných informácií na prípady, ktoré sú priamo relevantné a potrebné, aby mohol vykonať uvedený účel. Zároveň by si mal ponechať údaje iba po dobu potrebnú na splnenie tohto cieľa. Inými slovami, kontrolóri údajov by mali získať osobné údaje, ktoré skutočne potrebujú a mali by ich uchovávať len po dobu nevyhnutne potrebnú“⁸].

Osoba spracovávajúca údaje

„Entita, ktorá spracováva osobné údaje podľa pokynov kontrolóra údajov“ [[HYPERLINK \l "PRIPARE1_1" 9](#)].

Dátový subjekt

„Dátový subjekt je osoba, ktorej osobné údaje sa získavajú, uchovávajú alebo spracovávajú“¹⁰].

Legitímnosť spracovávania

„Legitímnosť spracovávania osobných údajov sa musí zaistiť buď na základe spracovávania údajov na základe súhlasu, zmluvy, právnej povinnosti, atď. Osobné údaje sa musia získať pre uvedené, explicitné a legitímne účely a nebudú sa ďalej spracovávať spôsobom nekompatibilným s týmito účelmi. Cieľ spracovávania by sa mal stanoviť najneskôr v momente získania údajov,“ [[HYPERLINK \l "PRIPARE1_1" 9](#)].

Osobné údaje alebo osobné identifikovateľné informácie (PII)

„Všetky informácie vzťahujúce sa na identifikovanú alebo identifikovateľnú fyzickú osobu (dátový subjekt); identifikovateľná osoba je osoba, ktorá sa dá identifikovať, priamo alebo nepriamo, najmä s odkazom na identifikačné číslo alebo jeden alebo viacero faktorov špecifických pre jej fyzickú, fyziologickú, duševnú, ekonomickú, kultúrnu alebo sociálnu identitu“⁴].

Súkromie

„Súkromie predstavuje schopnosť osoby zostať o samote, mimo verejnosti a pod kontrolou informácií o sebe. Môžeme rozlíšiť schopnosť prieniku do fyzického priestoru osoby („fyzické súkromie“, napríklad s ohľadom na ochranu súkromného majetku) a schopnosť kontrolovať získavanie a zdieľanie informácií o osobe („súkromie informácií“). Koncept súkromia s apreto prekrýva, ale nezhoduje, s konceptom ochrany údajov“ [[HYPERLINK \l "EDPSPrivacy" 11](#)].

Súkromie na základe projektu (PbD)

„Ide o prístup k ochrane súkromia zakódovaním v projektových špecifikáciách v rámci technológií, obchodných postupov a fyzickej infraštruktúry. To znamená budovanie súkromia smerom dopredu – priamo do projektových špecifikácií a architektúry nových systémov a procesov“¹²].

Technológia na podporu súkromia (PET)

„PET predstavuje kontrolu súkromia, ktorá pozostáva z opatrení informačných a komunikačných technológií (ICT), produktov alebo služieb, ktoré chránia súkromie elimináciou alebo znížením objemu osobne identifikovateľných informácií (PII) alebo prevenciou zbytočného a/alebo neželaného spracovávania PII, a to všetko bez straty funkčnosti systému ICT“ [[HYPERLINK \I "ISO29100" 2](#)].

Riadenie rizika súkromia

Proces riadenia rizika súkromia je „Reťazový proces, ktorý umožňuje objektívne riadiť riziká súkromia u dátových subjektov spojené so spracovávaním osobných údajov. V podstate pozostáva z ich hodnotenia (identifikácie, odhadu v zmysle závažnosti a pravdepodobnosti s hodnotením na porovnanie), ich posudzovanie (stanovenie a implementácia pomerných opatrení), prijímanie zvyškových rizík, komunikácia (konzultácia s účastníkmi, prezentácia výsledkov...) a monitorovanie zmien v čase (kontext, riziko, opatrenia...)“ 13].

Na základe riadenia rizík súkromia existujú niektoré základné koncepty, ktoré by sa tu mohli uviesť:

- Hrozba: „Typická činnosť používaná zdrojmi rizika, ktorá môže spôsobiť obávanú udalosť“ [[HYPERLINK \I "CNILPRM" 13](#)]
- Zraniteľnosť: „chyba alebo nedostatok postupov bezpečnosti a súkromia, projekt alebo implementácia produktu, ktorý by sa dal vykonávať a má za následok porušenie bezpečnosti alebo súkromia“ 14]
- Opatrenie alebo protiopatrenie: (technický alebo organizačný) mechanizmus alebo opatrenie pre zmeny/zníženie, zdieľanie/prenos alebo zachovanie rizika
- Riziko: „Scenár, ktorý popisuje obávanú udalosť a všetky hrozby, ktoré ju umožňujú. Odhaduje sa v zmysle závažnosti a pravdepodobnosti.“ [[HYPERLINK \I "CNILPRM" 13](#)]
- Zdroj rizika: „Osoba alebo iný ako ľudský zdroj, ktorý môže spôsobiť riziko, náhodne alebo zámerne“ 13]
- Závažnosť: „Odhad rozsahu potenciálnych vplyvov na súkromie dátových subjektov. V podstate závisí od miery identifikácie osobných údajov a predbežného vplyvu potenciálnych účinkov“ [[HYPERLINK \I "CNILPRM" 13](#)]

Súkromný účastník

„Fyzická alebo právnická osoba, verejný orgán, agentúra alebo iný orgán, ktorý môže ovplyvniť, byť ovplyvnený alebo ktorý s amôže vnímať ako ovplyvnený rozhodnutím alebo činnosťou spojenou so spracovávaním osobne identifikovateľných informácií (PII) processing“2].

Proportionalita

„Princíp proportionality v informačnej spoločnosti sa prejednal v právnom prípade Promusicae vs. Telefonica (C-275/06). Tento princíp si vyžaduje férovú rovnováhu medzi rôznymi základnými právami chránenými právnym poriadkom EÚ. Dodatočne, vo všeobecnej doktríne EÚ, existujú štyri kritériá pre overenie proporcionality opatrenia (test proportionality): musí existovať legitímny cieľ pre dané opatrenie, (ii) toto opatrenie musí byť vhodné na dosiahnutie cieľa, (iii) toto opatrenie musí byť potrebné na

dosiahnutie cieľa, (iv) toto opatrenie musí byť rozumné, keď vezmeme do úvahy konkurenčné záujmy. Európsky súdny dvor (ECJ) často zlučuje dve posledné kritériá do jedného" [[HYPERLINK \I "PRIPARE1_1" 9](#)].

Pseudonymita

„Pseudonymita zaistuje, že používateľ môže používať zdroj alebo službu bez zverejnenia svojej identity, stále však zostáva zodpovedný za toto používanie. Používateľ môže byť zodpovedný tým, že bude priamo spojený s referenciou (aliasom) cieľa hodnotenia bezpečnostných funkcií alebo poskytnutím aliasu, ktorý sa použije na účely spracovávania, ako je číslo účtu“15].

Polovičný identifikátor

„Sústava atribútov, ktoré môžu byť v kombinácii spojené s externými informáciami pre opätovnú identifikáciu (alebo zníženie neistoty) všetkých alebo niektorých respondentov, na ktorých sa tieto informácie vzťahujú“ [[HYPERLINK \I "LeM07" 14](#)]. Napr. „Osoba sa neidentifikuje ani podľa pohlavia, rodného čísla ani PSČ, ale kombinácia týchto troch údajov je postačujúca na identifikáciu 87 % v Spojených Štátoch“16].

Citlivé osobné údaje alebo citlivé PII

Aktuálna smernice EÚ o ochrane údajov [[HYPERLINK \I "Eur951" 4](#)] uvádza, ktoré kategórie osobných údajov sa považujú na základe svojej podstaty za citlivé (náboženstvo, politické názory, zdravie, sexuálna orientácia, rasa a členstvo v minulých organizáciách) a aké špeciálne opatrenia sa musia prijať pri spracovávaní týchto údajov. V novom nariadení EÚ o ochrane údajov sa môžu pridať nové kategórie ako je rodová identita, biometrické údaje, administratívne sankcie, podozrenie na priestupky alebo filozofické presvedčenie.

7 Analýza a hodnotenie existujúcich prístupov PbD

Súkromie v projekte je prezentované v publikácii Ann Cavoukian¹⁷] a „uznáva sa ako základný komponent základnej ochrany súkromia“ [[HYPERLINK \l "32n10" 18](#)] v roku 2010. Aj napriek jej medzinárodnej podpore sa tento prejav kritizoval ako „nejasný“ a považoval sa za ťažko pretaviteľný do praxe¹⁹].

Avšak a na základe toho, že PbD, podľa definície od Cavoukian, nie je vôbec praktický, existuje viacero postupov spojených s princípmi PbD, ktoré sa dajú dodržiavať, aby sa skutočne zvýšila miera súkromia počas budovania a prevádzky nových systémov. V nasledujúcich podriadených častiach predstavujeme najrozšírenejšie a najrelevantnejšie prístupy, ktoré zdôrazňujú ich výhody a nevýhody.

7.1 Princípy súkromia

Došlo k mnohým celosvetovým pokusom o zachytenie univerzálneho pohľadu na súkromie a jeho prenos do legislatívy alebo všeobecných princípov (napr. FIPP, Smernica EÚ o ochrane údajov, OECD, atď. Súkromie je však veľmi komplexným subjektom, keďže do značnej miery závisí od kontextu a očakávaní dátového subjektu, ktoré sú úzko spojené s oblasťou, kontextom a účelom údajov zachytených kontrolórom údajov.

Ak sa chcete zamerať na túto subjektivitu, namiesto dodržiavania úzkeho zoznamu princípov Finn et al. navrhuje uplatniť systematiku súkromia [[HYPERLINK \l "Rac13" 20](#)], ktorá sa dá použiť na navigáciu a zdôvodnenie súkromia a potenciálnych problémov u príslušných účastníkov. Navrhovaná systematika je postavená na siedmych typoch súkromia: súkromie osoby, súkromie správania a činnosti, súkromie komunikácie, súkromie údajov a imidžu, súkromie myšlienok a pocitov, súkromie miesta a priestoru a súkromie združovania

Nakoľko princípy súkromia sú užitočné ako ciele vysokej úrovne systému ICT a systematika poskytuje dobrý počiatočný bod pre identifikáciu potenciálnych otázok súkromia a diskusiu s účastníkmi, tieto samostatné zoznamy sú obvyčajne zostavené pomocou právneho jazyka a nie sú priamo použiteľné z pohľadu technológie.

7.2 Hodnotenia vplyvu na súkromie (PIA)

Krok vpred pre využiteľnosť princípov súkromia, ich pochopiteľnosť a použiteľnosť v technickej oblasti systému predstavovali šírenie rámcov PIA.

Hodnotenie vplyvu na súkromie podľa Clarke²¹] predstavuje „systematický proces hodnotenia potenciálnych vplyvov na súkromie projektu, iniciatívu alebo navrhovaný systém alebo schému“, čo predstavuje koncept, s ktorým sa spájajú inžinieri systému.

Hoci PIAs predstavujú koncept, ktorý bol zavedený už v 90-tych rokoch v anglosaských krajinách, najvýznamnejšie udalosti spojené s prijatím hlavného prúdu PIA v Európe sú relatívne nové:

- 2007: Kancelária informačného komisára UK (ICO) zverejnila príručku PIA (ktorá bola zrevidovaná v júni 2009 [[HYPERLINK \I "ICO09" 22](#)]), prvú svojho druhu v Európe.
- 2011: Odvetvie RFID samostatne zverejnilo (na základe odporúčania EC) svoj vlastný rámec hodnotenia vplyvu na ochranu údajov na pomoc operátorom aplikácie RFID pri odhaľovaní rizík súkromia 23].
- 2011: Bundesamt für Sicherheit in der Informationstechnik (BSI) zverejnil svoju vlastnú metodológiu PIA [[HYPERLINK \I "Bun11" 24](#)], podrobný popis veľmi generického procesu uvedeného v rámci RFID PIA23]
- 2012: EC do svojho návrhu na nariadenie EÚ o ochrane údajov [[HYPERLINK \I "Eur2" 25](#)] v článku 33 zapojila povinné hodnotenie vplyvu na ochranu údajov pre organizácie z verejného a súkromného sektora v Európe („pre spracovávanie predstavujú operácie špecifické riziká pre práva a slobody dátových subjektov na základe ich podstaty, rozsahu a cieľov“)
- 2014: UK ICO zverejnil svoj kódex postupov na vykonávanie hodnotení vplyvu na súkromie22]
- 2015: CNIL zverejnil svoju metodológiu hodnotenia vplyvu na súkromie [[HYPERLINK \I "Com" 26](#)]

PIAF, projekt financovaný EC (ktorý sa skončil v roku 2012), mal za cieľ zhodnotiť viaceré rámce PIA a správy, aby identifikoval najlepšie postupy v oblasti PIA. Na záver tento projekt zverejnil sústavu krokov a odporúčaním, ktoré by mal proces PIA dodržiavať 27]:

1. Určiť, či je PIA potrebný
2. Identifikovať tím PIA a stanoviť referenčné podmienky, zdroje a časový rámec
3. Pripraviť plán PIA
4. Stanoviť rozpočet pre PIA
5. Popísať navrhovaný projekt, ktorý sa zhodnotí
6. Identifikovať účastníkov
7. Popísať informačné toky a iné vplyvy na súkromie
8. Konzultovať s účastníkmi
9. Overiť, či sa projekt zhoduje s legislatívou
10. Identifikovať riziká a možné riešenia
11. Formulovať odporúčania
12. Pripraviť a zverejniť správu
13. Implementovať odporúčania
14. Revízia tretej strany a/alebo audit PIA
15. Aktualizácia PIA, ak dôjde ku zmenám v projekte
16. Kódovať povedomie o súkromí v organizácii a zaistiť zodpovednosť.

Aj napriek tomu, že PIAs predstavujú krok vpred pre skutočné uvedenie do prevádzky a zavedenie súkromia do systémov, PIAs majú stále isté medzery, ktoré je potrebné pokryť:

- Nie sú spojené s rozšírenými procesmi technického rozvoja (e.g. Scrum, Iterative, Waterfall...);
- Identifikácia rizík je skôr komplexnou úlohou. Požadujú sa konkrétnejšie odporúčania alebo špecifické metodológie hodnotenia rizík
- Nemajú reťazovú perspektívu. Teda odporúčanie na riešenie špecifických rizík môže vytvárať nové riziká, ktoré by sa museli zhodnotiť, prejednať s účastníkmi... Musí byť jasné, že PIA nie sú lineárnym procesom, ale reťazovým procesom.

- Neobsahujú architektonický rozmer systému.
- Nepokrývajú celý technický životný cyklus (teda rozvoj).
- Existuje riziko, že sa PIA zmenia jednoducho na kontroly právnej zhody.

7.3 Organizácia pre napredovanie noriem štruktúrovaných informácií (OASIS)

OASIS má dve hlavné iniciatívy noriem, ktoré podporujú súkromie a ktoré sú úzko spojené so súkromím v projekte:

- Referenčný model riadenia súkromia (PMRM) [[HYPERLINK \I "PMRM" 28](#)]: Hlavným cieľom PMRM, podľa jeho najnovšieho návrhu (z júla 2013) je:
 - „pochopiť a analyzovať politiky súkromia a ich požiadavky riadenia súkromia v stanovených prípadoch používania; a
 - Zvoliť technické služby, ktoré sa musia implementovať pre podporu kontroly súkromia.“
- Súkromie na základe projektovej dokumentácie pre softvérových inžinierov (PBD-SE): „poskytuje riadenie súkromia a normy dokumentácie pre softvérových inžinierov. Umožňuje softvérovým organizáciám kódovať súkromie do projektu a architektúry IT systémov, bez zmenšenia funkčnosti systému“²⁹]

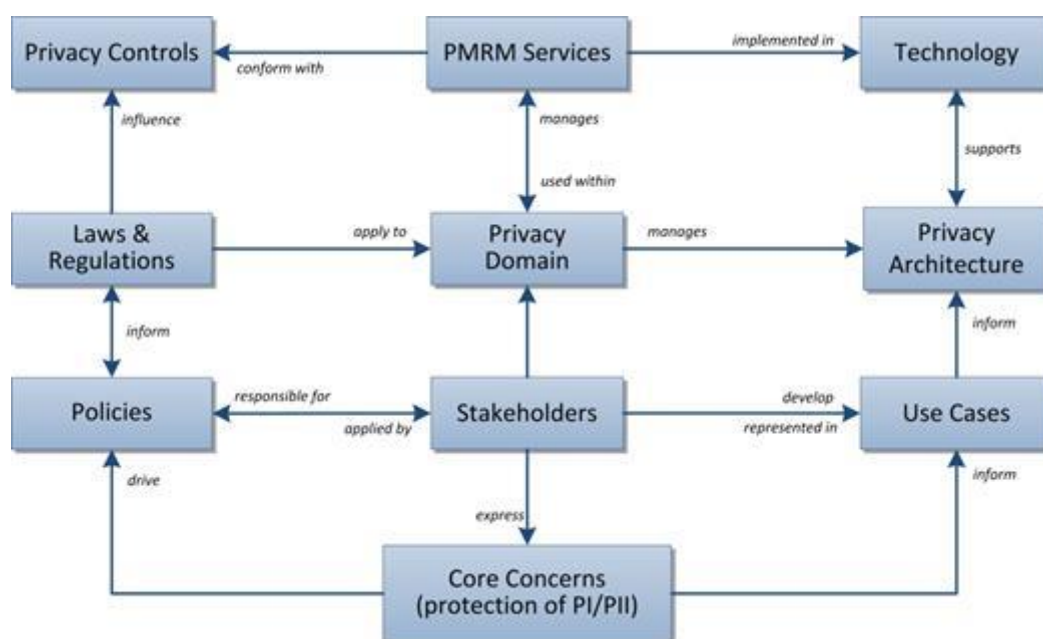
7.3.1 PMRM

PMRM, ktorý môže nahradiť PIAs, nie je kompletným zoznamom procesov, ktoré by sa mali prijať ako celok. Na druhej strane, účastníci by mali prijať a upraviť niektoré body metodológie organizácie a procesy na vypracovanie systému. Metodológia PMRM je určená nielen pre systém a obchodných analytikov a projektantov, je významná aj ako komunikačný prostriedok s úradníkmi pracujúcimi v oblasti súkromia a rizík, orgánmi pre ochranu údajov a politikmi. PMRM je založený na vlastnej sústave prevádzkových féroých informačných postupov/princípov („FIPPs“) odvodených od revízie relevantných medzinárodných legislatívnych nástrojov.

PMRM je postavený na 3 pilieroch. V prvom rade na referenčnom modeli, ktorý spája hlavné koncepty spojené so súkromím a technické koncepty systému. V druhom rade na samotnej metodológii, ktorá sa skladá z viacerých úloh, ktoré sú jasne a stručne popísané. A napokon na sústave prevádzkových služieb, ktoré slúžia na mapovanie identifikovaných kontrol súkromia u implementovaných mechanizmov.

Referenčný model

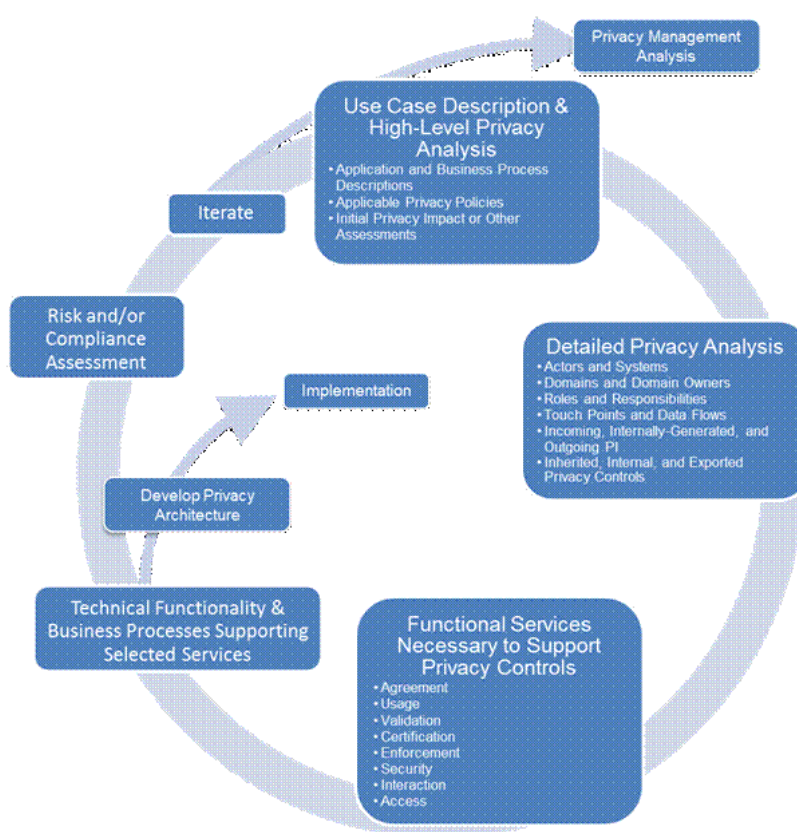
PMRM obsahuje glosár výrazov a referenčný model, ktoré pomáhajú vypracovať základnú terminológiu, ktorá sa bude používať medzi účastníkmi a ktorá zlepší komunikáciu medzi ľuďmi s rôznymi profesionálnymi oblasťami alebo vzdelaním. Zároveň slúži ako štandardný koncepčný model súkromia, ktorý sa dá použiť na účely vzdelávania.



Obrázok1: Konceptný model PMRM [[HYPERLINK \I "PMRM" 28](#)]

Metodológia

PMRM od začiatku zdôrazňuje, že ide o REŤAZOVÚ metodológiu, ktorá potvrdzuje komplexnosť súkromia a spôsobu, akým sa musia dodržiavať viaceré opakovania, zdokonalenia, úpravy a výber kontrol súkromia.



Obrázok 2: Prehľad metodológie PMRM [28]

Táto metodológia je rozdelená na šesť hlavných fáz, ktoré sú rozdelené na jednotlivé úlohy s jasnými cieľmi a očakávanými výstupmi. Rozsiahle zoznamy úloh a cieľov nájdete v popise metodológie, je však vhodné uviesť aj zoznam najvýznamnejších cieľov:

- „Ohodnoťte aplikáciu alebo obchodnú službu, s ktorou sú spojené osobné informácie (PI) - v podstate ide o identifikáciu kompletného prostredia, v ktorom sa dá použiť aplikácia alebo schopnosti a požiadavky ochrany údajov.“
- „Pripravte a zdokumentujte podrobnú analýzu riadenia súkromia prípadu používania, ktorá zodpovedá analýze súkromia na vysokej úrovni a popisu prípadu používania na vysokej úrovni“
- „Identifikujte pri každej výmene toku osobných údajov medzi systémami prevádzkové služby potrebné na podporu prevádzky predtým identifikovaných kontrol súkromia“

Prevádzkové služby

PMRM poskytuje sústavu ôsmich prevádzkových služieb, ktoré sa dajú použiť na spájanie požadovaných kontrol súkromia pri prevádzkových mechanizmoch potrebných na implementáciu týchto požiadaviek:

Služba	Funkcia	Účel
Dohoda	Zadefinovať a zdokumentovať povolenia a pravidlá pre spracovávanie osobných údajov na základe platnej politiky, preferencií dátového subjektu a iných relevantných faktorov; poskytnúť relevantným aktérom mechanizmus na vyjednávanie alebo stanovenie nových povolení a pravidiel; vyjadrenie dohôd na používanie inými službami	Riadiť a vyjednať povolenia a pravidlá
Používanie	Zaistiť, aby bolo používanie osobných údajov v súlade s podmienkami platného povolenia, politiky, zákona alebo nariadenia, vrátane osobných údajov podliehajúcich minimalizácii informácií, spájaniu, integrácii, úsudkom, prenosu, odvodzovaniu, spájaniu a anonymizácii životného cyklu prípadu používania	Kontrolovať používanie osobných údajov
Potvrdenie	Zhodnotiť a zaistiť kvalitu informácií osobných údajov v zmysle presnosti, kompletnosti, relevantnosti, včasnosti a iných príslušných kvalitatívnych faktorov	Overiť osobné údaje
Certifikácia	Zaistiť, aby prihlasovacie údaje aktéra, domény, systému alebo komponentu systému boli kompatibilné s pridelenými úlohami v oblasti spracovávania osobných údajov; a overiť ich zhodu a dôveryhodnosť na základe zadaných politiky a pridelených úloh.	Overiť prihlasovacie údaje
Vynútenie	Spustiť činnosti odpovede, vykonávania politiky a rekurzu vtedy, keď kontroly auditu a monitorovania indikujú, že sa aktér alebo systém nezhoduje so stanovenou politikou alebo s podmienkami povolenia (dohody)	Monitorovať a odpovedať na auditované podmienky výnimiek
Bezpečnosť	Poskytnúť procesné a technické mechanizmy potrebné pre dôvernú, integritu a dostupnosť osobných	Chrániť súkromné

Služba	Funkcia	Účel
	informácií; umožniť dôveryhodné spracovanie, komunikáciu, ukladanie a používanie operácií súkromia	informácie a operácie
Interakcia	Poskytnúť všeobecné rozhrania potrebné na prezentáciu, komunikáciu a interakciu osobných údajov a príslušných informácií spojených s osobnými údajmi; zahŕňa funkciu, ako sú používateľské rozhrania, medzisystémové výmeny informácií a agenti	Prezentácia informácií a komunikácia
Prístup	Povoliť dátovým subjektom, podľa požiadavky a/alebo na základe povolenia, politiky alebo nariadenia, kontrolovať ich PI, ktorý sa nachádza v danej oblasti a navrhnúť zmeny a/alebo korekcie osobných údajov	Pozerať a navrhovať zmeny uložených osobných údajov

Tabuľka 1: Prevádzkové služby PMRM [28]

PMRM je krokom vpred v oblasti budovania súkromia, presahuje „tradičné“ PIAs. Najvýznamnejšie body PMRM sú:

- Reťazový prístup.
- Komplexná, ale jednoduchá stručná metodológia, vrátane príkladov pre zjednosušenie jej prijímania.
- Odkazuje na a spája sa riadením rizika a prístupmi PIA.
- Poskytuje systematiku služby, ktorá môže byť užitočná pre neskúsených účastníkov.

Aj napriek úsiliu PMRM tu ešte stále existujú medzery, ktoré sa musia riešiť, pred zavedením kompletnej technickej metodológie systému súkromia:

- Neobsahuje architektonický rozmer systému, ktorý je kľúčovým aspektom pre budovanie súkromia;
- Nie je spojený s rozšírenými procesmi technického rozvoja (napr. SCRUM, Iterative, Waterfall...);
- Identifikácia rizík je skôr komplexnou úlohou. Požadujú sa konkrétnejšie odporúčania alebo špecifické metodológie hodnotenia rizík
- Nepokrýva celý životný cyklus systému (teda rozvoj).
- PMRM by značne využíval poskytnutie rozsiahleho zoznamu mechanizmov súkromia, ktoré budú riešiť spoločné kontroly alebo požiadavky súkromia;

7.3.2 PBD-SE

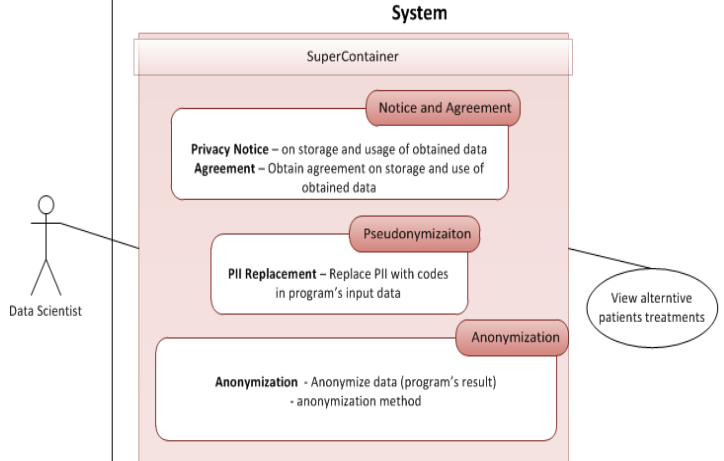
OASIS PbD-SE Hlavným cieľom technického výboru je poskytnúť „pomoc a požiadavky pre inžinierov pre zdokumentovanie cieľov súkromia a príslušných kontrolných opatrení v rámci cyklu životnosti rozvoja softvéru“. Medzi príklady týchto foriem dokumentácie patria:

- Zoznamy,

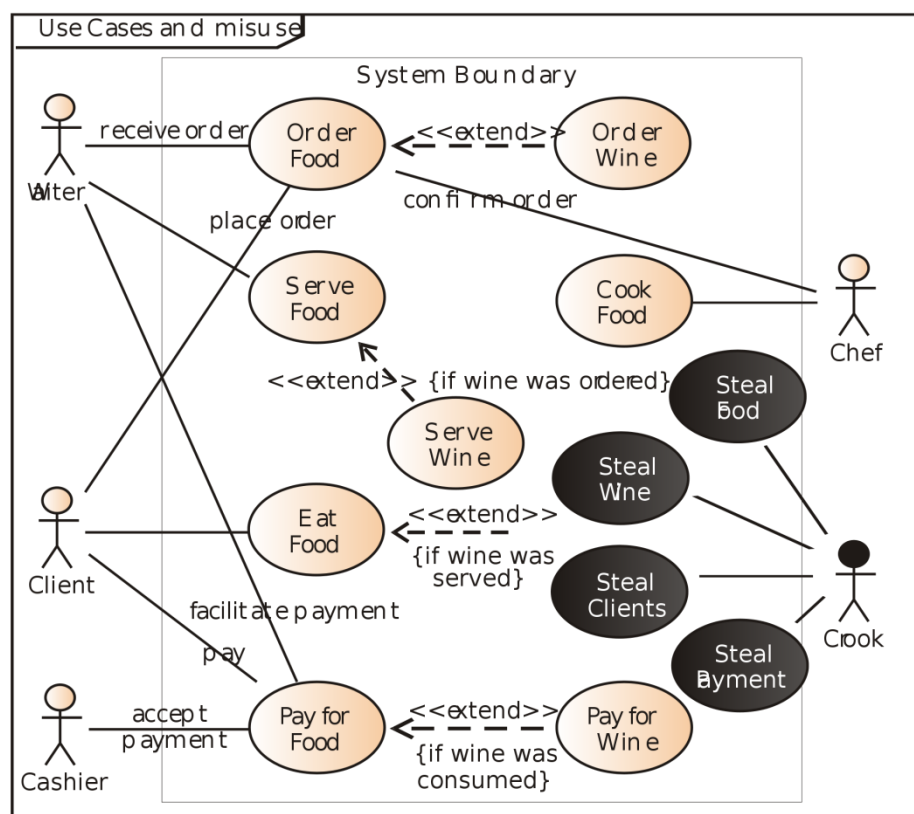
- DFD,
- Príbehy používateľov,
- UML (napr. trieda, tok údajov, sekvencia, diagramy aktivity).

PbD-SE TC má dve rôzne pracovné línie. V jednej pracuje na základe „sústavy smerníc pre normu, ktorá kóduje súkromie priamo do fázy analýzy a projektovej fázy rozvoja projektu“ **Error! Reference source not found.**, ako je „Stanovenie dokumentácie spojenej s cieľmi súkromia alebo požiadavkami, ktoré splnia 7 Základných princípov pľ PbD (Pbd-SE**Error! Reference source not found.**, Tabuľka 2.1)“ alebo „Zaistenie toho, aby sa súkromné služby (napr. pre audit, používanie údajov, potvrdenie, bezpečnosť) integrovali do artefaktov diagramu komunikácie ako sú diagramy scenára“.

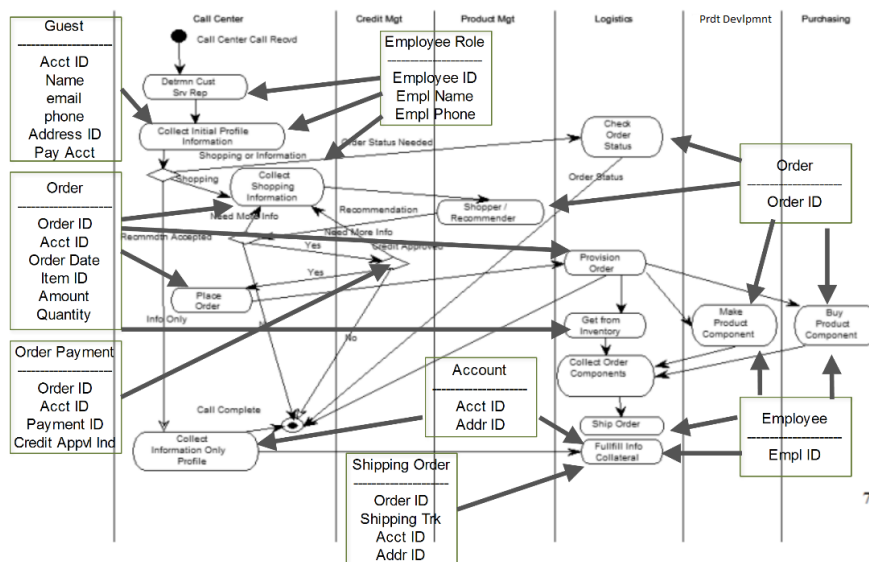
Na druhej strane sa PbD-SE navrhuje ako úsilie o vypracovanie normy pre procesy riadenia a dokumentáciu technických artefaktov vyvolaných súkromím pri analýze softvérových systémov a úrovniach dizajnu. PbD-SE pracuje na vypracovaní dokumentácie súkromia, vrátane nástrojov a vizuálnych modelov súkromia. Napr.:

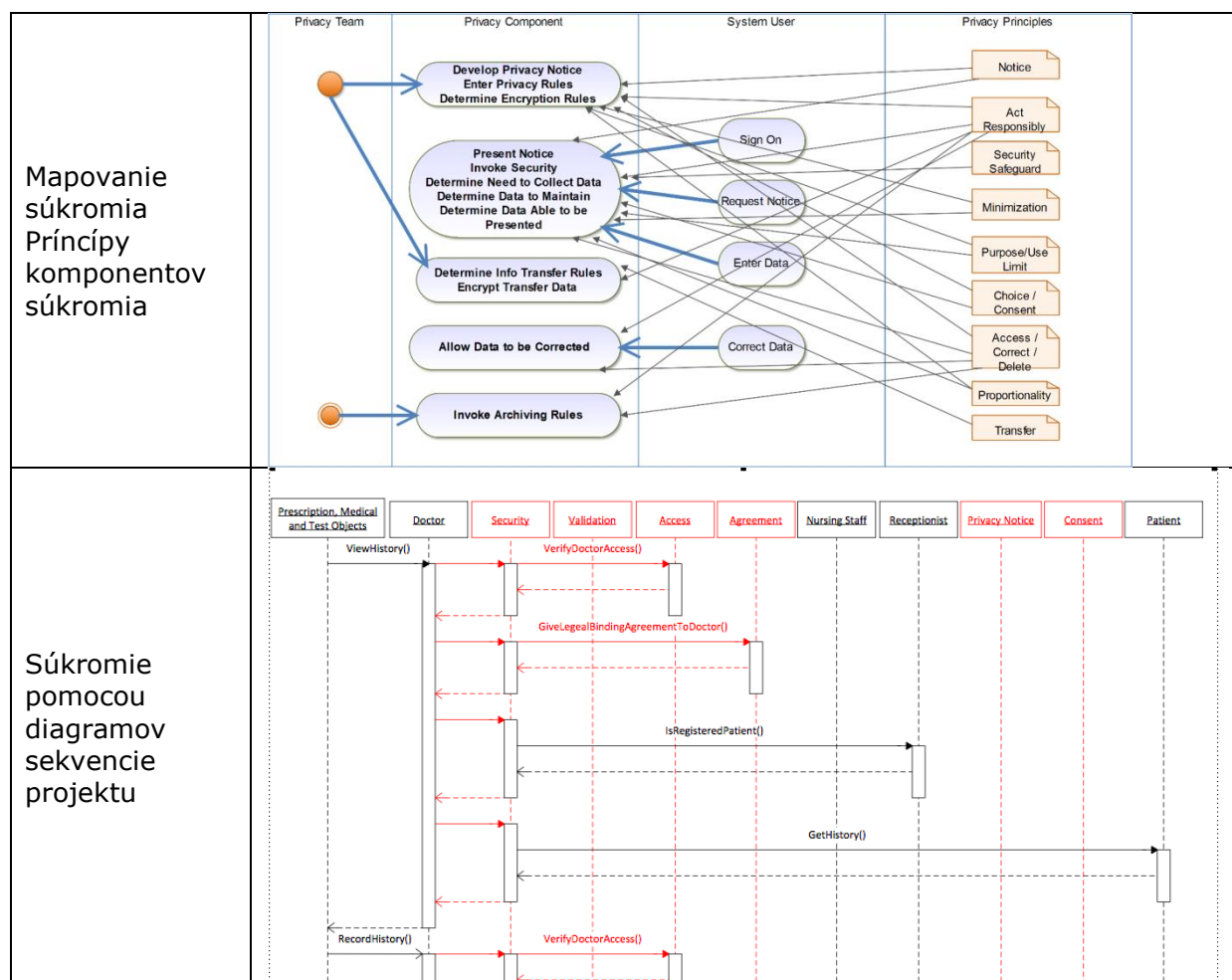
Súkromie pomocou šablóny prípadu používania projektu pre požiadavky súkromia	Napr. šablóna založená na PMRM: • Názov prípadu používania • Kategória prípadu používania • Popis prípadu používania • Aplikácie spájané s prípadom používania • Dátové subjekty spájané s prípadom používania • PI a PII a právne, regulačné a/alebo obchodné politiky riadiace PI a PII v prípade používania • Domény, vlastníci domén a úlohy spojené s prípadom používania • Dátové toky a dotykové body spájajúce domény alebo systémy • Systémy podporujúce aplikácie prípadu používania • Kontroly súkromia požadované pri implementácii developera • Služby
Diagram prípadu používania so službami súkromia pri implementácii kontrol	

Súkromie
pomocou
diagramov
prípadu
nesprávneho
používania
projektu



Súkromie
pomocou
projektu a
diagramov
aktivity





Tabuľka 2: Príklady dokumentácie a vizuálne modely súkromia

PbD-SE nie je samostatným prístupom, ale funguje ako vynikajúci doplnok k ostatným prístupom PbD (napr. PIAs alebo PMRM), čo poskytuje sústavu prostriedkov pre dokumentáciu požiadaviek každého nového systému a zároveň pre technický proces PbD.

7.4 Metodológie hodnotenia rizík súkromia

Homologické pre implementáciu metodológií pre riadenie bezpečnostného rizika, ktoré tu existuje od roku 1974 **Error! Reference source not found.**, metodológie hodnotenia rizika súkromia sa objavili v priebehu niekoľkých minulých rokov. Tieto inovatívne metodológie hodnotenia rizík súkromia riešia koncepty, princípy, hrzby a kontroly špecifické pre súkromie.

Hlavnou výhodou používania prístupu riadenia rizika na riešenie súkromia počas projektu systému je to, že okrem pomoci pri identifikácii aktív, ktoré sa majú chrániť a hrozieb, ktoré ohrozujú takéto aktíva, pomáha prioritizovať riziká pri zohľadnení ich pravdepodobnosti a potenciálneho vplyvu.

Nasledujúci obrázok ukazuje hlavné fázy všeobecného **retázového** procesu riadenia rizika:



Obrázok 3: Fázy riadenia rizika

Fáza	Ciele
Identifikácia	- Charakterizácia systému - Identifikácia hrozieb - Identifikácia zraniteľných bodov
Analýza	- Stanovenie pravdepodobnosti hrozieb - Stanovenie vplyvu činností hrozieb - Stanovenie miery rizika
Plánovanie	- Identifikácia a výber kontrol, ktoré znížia pravdepodobnosť alebo vplyv hrozieb - Plánovanie zapojenia takýchto kontrol do fáz dizajnu a implementácie
Sledovanie	Zaistenie zavedenia plánovaných kontrol a účinného zníženia rizík
Dokumentácia	- Dokumentácia príslušných rizík a ich vzťahov so zvolenými kontrolami - Znížené riziká môžu mať istú zostávajúcu pravdepodobnosť a vplyv. Operátorom systému a majiteľom by to zároveň malo byť jasné

Obrázok 4: Fázy a ciele riadenia rizika

Kedže existuje istá dohoda s týmto všeobecným pohľadom na proces riadenia rizika, každý rámec alebo metodológia má svoj vlastný pohľad a zameriava sa na niektoré aspekty tohto všeobecného modelu.

Ďalším odlišujúcim aspektom rámcov hodnotenia rizika súkromia alebo metodológií je spôsob merania vplyvu, náročný aspekt vyplývajúci z vysokej miery subjektivity, ktorá sa vzťahuje na súkromie.

Ďalej bude metodológia rizika súkromia vysvetlená s istou mierou podrobností a ďalšie prístupy rizika súkromia sa zhodnotia v porovnaní s CNIL jeden.

7.4.1 Metodológia rizika súkromia CNIL

Francúzska národná komisia informatiky a slobody (Commission nationale de l'informatique et des libertés – CNIL) predstavila v roku 2012 rámec riadenia rizika

súkromia **Error! Reference source not found.**, odvodený od jej bezpečnostného rámca (Expression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité - EBIOS).

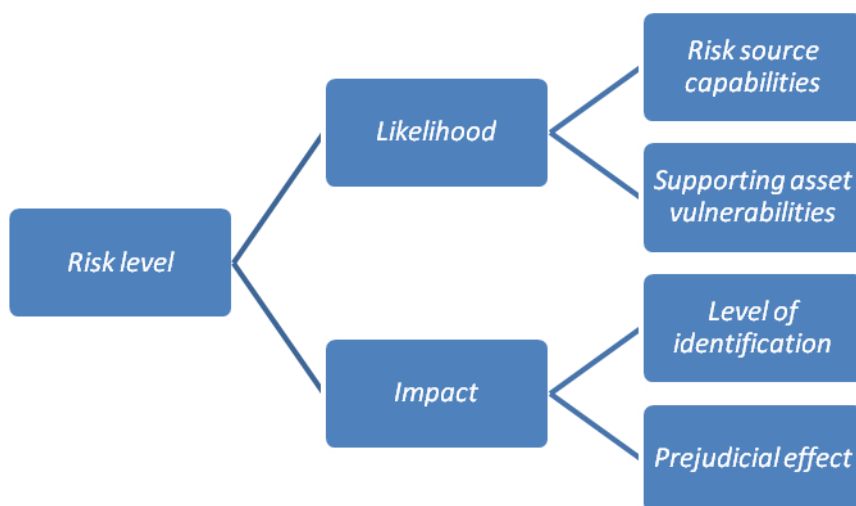
Prístup metodológie rizika súkromia CNIL pozostáva z 5 hlavných fáz:

Základná štúdia

Pochopte kontext spracovávaní osobných údajov. Táto fáza obsahuje identifikáciu a charakterizáciu operácií spracovávaní s potenciálnymi rizikami súkromia: jej účel, pre koho je určená, príslušné obchodné procesy, **ovplyvnené dátové subjekty, príslušné právne procesy a všetky zapojené osobné údaje**.

Štúdia obávaných udalostí

„Cieľom tejto fázy je získať podrobný a prioritný zoznam všetkých obávaných udalostí, ktoré môžu ovplyvniť príslušnú operáciu spracovávaní“. Obávané udalosti sa musia zaradiť podľa svojej úrovne rizika, ktorá sa vyráta pomocou viacerých faktorov znázornených na Obrázku 5.



Obrázok 5: Model stanovenia miery rizika CNIL

Pri každej identifikovanej hrozbe (aktivita podporená zoznamom hrozieb uvedeným v prílohe metodológie) analytik, v **spolupráci so všetkými zapojenými účastníkmi**, musí identifikovať jej potenciálny vplyv v neželanom prípade, kedy sa táto obávaná udalosť prejaví.

CNIL navrhuje stanoviť vplyv obáwanej udalosti pri zohľadnení toho aké bude jednoduché identifikovať príslušné dátové subjekty a negatívny vplyv takejto identifikácie. Obidva parametre (miera identifikácie a negatívne vplyvy) sa musia odhadnúť pomocou škály od 1 do 4 (zanedbateľný - maximálny) a príslušná závažnosť sa vyráta pomocou nasledujúceho vzorca:

Miera identifikácie + negatívne vplyvy Príslušná závažnosť	Príslušná závažnosť
<5	1. Zanedbateľná
=5	2. Obmedzená
=6	3. Významná

> 6	4. Maximálna
-----	--------------

Tabuľka 3: Vzorec závažnosti CNIL

Nasledujúca tabuľka uvádza príklad identifikovaných obávaných udalostí a spôsob odhadu závažnosti:

Obávaná udalosť	Miera identifikácie osobných údajov	Závažnejšie potenciálne vplyvy	Negatívne vplyvy potenciálnych vplyvov	Maximálna závažnosť
Nelegitímny prístup k osobným údajom	4. Maximálna	- Krádež účtu - Používanie na obchodné účely	3. Významná	4. Maximálna

Tabuľka 4: Príklad výpočtu závažnosti CNIL

Štúdia hrozieb

Po vypočítaní zoznamu obávaných udalostí a jeho potenciálnej závažnosti je nasledujúcim krokom identifikácia všetkých hrozieb, ktoré môžu umožniť výskyt obávaných udalostí. Pri každej hrozbe CNIL navrhuje pozrieť sa na aktíva, ktoré podporujú systém, ktorý je predmetom štúdie a zhodnotí jeho zraniteľnosť. Druhým krokom je odhad schopností zdrojov rizika, ktoré môžu zneužiť túto zraniteľnosť. Vzorec podobný vzorcu použitému na výpočet závažnosti sa navrhuje aj na odhad pravdepodobnosti:

podpora zraniteľnosti aktív + schopnosti zdroja rizika	Príslušná pravdepodobnosť
<5	1. Zanedbateľná
=5	2. Obmedzená
=6	3. Významná
> 6	4. Maximálna

Tabuľka 5: Vzorec odhadu pravdepodobnosti CNIL

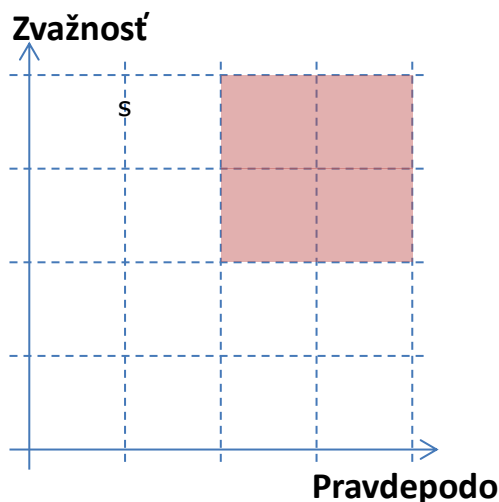
Nasledujúca tabuľka uvádza príklad identifikovaných obávaných udalostí a spôsob odhadu pravdepodobnosti:

Obávaná udalosť	Najpravdepodobnejšie hrozby	Podpora zraniteľnosti aktív	Schopnosti zdrojov rizík	Maximálna pravdepodobnosť
Nelegitímny prístup k osobným údajom	- Krádež hardvéru (napr. krádež laptopu vo vlaku) - Porucha funkcie softvéru (napr. pri osobnom použití) - Zmena softvéru (napr.: šírenie vírusov)	3. Významná	3. Významná	3. Významná

Tabuľka 6: Príklad výpočtu pravdepodobnosti CNIL

Štúdia rizika

Jej cieľom je získať mapu rizika pre prioritizáciu rizík, ktoré sa musia riešiť. CNIL navrhuje nasledujúcu mriežku pre mapu:



Tabuľka 7: Návrh CNIL na mapu rizika

Štúdia opatrení

Cieľom tejto fázy je vybrať a identifikovať kontroly, ktoré dokážu znížiť pravdepodobnosť alebo zvažnosť obávaných udalostí. Tieto opatrenia sa dajú zvoliť z existujúcich zoznamov opatrení alebo dobrých postupov alebo sa môžu navrhnúť pre daný systém ad-hoc

Jednoznačne dôležité je identifikovať zvyškové riziká, ktoré zostanú aj po naplánovaní preniknutia zvolených a pre spojenie jednotlivých opatrení s obávanými udalosťami a hrozbami, ktoré sú ovplyvnené daným opatrením.

V júni 2015 CNIL nahradil svoju metodológiu rizika súkromia za komplexnú metodológiu (ktorá obsahuje metodológiu rizika súkromia) a poskytol pomoc pri vykonávaní celého PIA **Error! Reference source not found.**

7.4.2 LINDDUN

Rovnakým spôsobom, akým sa metodológia rizika súkromia CNIL prejavila v bezpečnostne orientovanej metodológii (EBIOS), LINDDUN **Error! Reference source not found.** presúva metodológiu STRIDE **Error! Reference source not found.** do oblasti súkromia.

LINDDUN pozostáva zo šiestich krokov, ktoré pomáhajú analytikom identifikovať problémy súkromia a systematicky si zvoliť vhodné opatrenia.



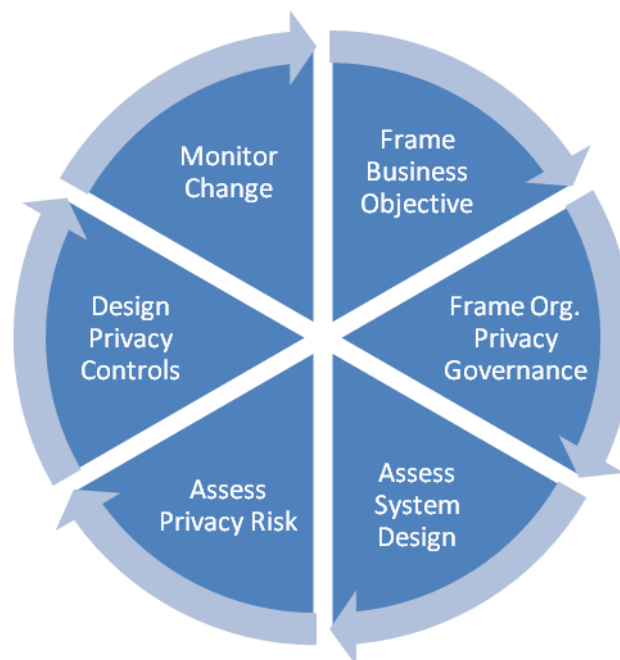
Obrázok 6: 6 krokov LINDDUN

V prvom rade by sme mali uviesť, že metodológie CNIL a LINDDUN sa zameriavajú na odlišné aspekty riadenia rizika súkromia a môžu byť doplnujúce. Zatiaľ čo LINDDUN robí dobrú prácu v oblasti systematickej identifikácie hrozieb, neposkytuje prostriedok pre prioritizáciu identifikácie hrozieb, ktorá predstavuje jednu z výhod metodológie CNIL. Mali by sa zdôrazniť niektoré kľúčové aspekty z LINDDUN:

- Na základe používania vizuálnych znázornení systému (DFD). Pomáha to analytikom lepšie znázorniť hrozby;
- Zapojenie kategorizácie hrozieb, ktoré sa dajú systematicky používať na všetky toky, procesy, sklady údajov a entity.
- Zverejnenie stromového katalógu hrozieb súkromia **Error! Reference source not found.**, ktorý identifikuje udalosti, ktoré môžu umožniť výskyt hrozby.
- Zverejnenie katalógu stratégií znižovania **Error! Reference source not found.** a PET spojených so stromovým katalógom súkromia

7.4.3 Návrh riadenia rizika súkromia NIST

V máji 2015 NIST zverejnil návrh **Error! Reference source not found.**, ktorý popisuje rámec riadenia rizík pre federálne informačné systémy (PRMF), ktoré si vyžadujú komentáre hľadajúce skúsenosti a perspektívy odborníkov na súkromie a používanie rôznych pozadí.



Obrázok 7: Rámec riadenia rizika súkromia NIST (PRMF)

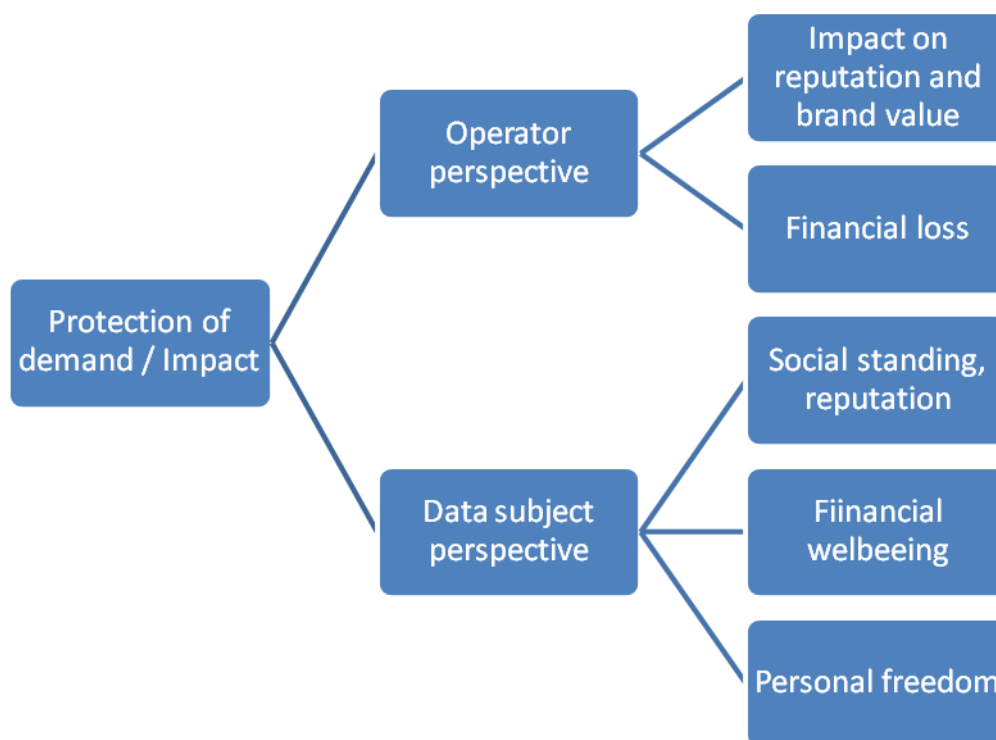
Zatiaľ čo prístup NIST nie je až taký odlišný od ostatných uvedených prístupov (ako je prístup CNIL) (pozrite si Obrázok 7), existujú niektoré pozitívne aspekty a medzery, ktoré by sa mali zdôrazniť a riešiť.

- Namiesto zamerania sa na rozvoj princípov súkromia sa zameriava na rozvoj troch cieľov súkromia „za účelom zjednodušenia rozvoja a prevádzky informačných systémov chrániacich súkromie: predvídateľnosť, ovládateľnosť a nezlúčiteľnosť.
- V modeli popísanom v PRMF, pri zohľadnení rizík súkromia, ktoré môžu ovplyvniť dátové subjekty, sa vplyv meria na organizačnej úrovni, pričom sa odstráni vplyv takýchto rizík na dátové subjekty.
- Nespája sa s iným úsilím alebo prístupmi ochrany súkromia (napr PIAs)
- Pozitívnym bodom je to, že riadi koncept „preukázania uvedenej funkcie ochrany súkromia“ ako obchodný cieľ.
- Neuvádza reťazovú podstatu procesu riadenia rizika, čo je negatívnym bodom.

7.4.4 BSI PIA

Zatiaľ čo smernica hodnotenia vplyvu na súkromie zverejnená v „Bundesamt für Sicherheit in der Informationstechnik“ už bola uvedená v časti 7.2, v tejto časti je vhodné uviesť jej prístup k meraniu miery rizika hrozieb súkromia.

BSI dodržiava „pozitívny“ prístup a namiesto rozprávania o „obávaných udalostiach“, ktorým je potrebné sa vyhnúť, hovorí o „cieľoch súkromia“, ktoré sa musia dosiahnuť. Tieto ciele sa hodnotia v zmysle svojej „potreby ochrany“ rovnako ako obávané udalosti, ktoré sa hodnotia na základe ich potenciálneho vplyvu v ostatných rámcoch hodnotenia rizík. Novinkou tohto prístupu BSI je to, že používa dve hlavné stanoviská a viacero faktorov na meranie tejto „potreby ochrany“, ktoré vidíme ako potenciálny negatívny vplyv nedosahovania cieľov:



Obrázok 8: Rozklad vplyvu BSI

Tento prístup obsahuje a vyvažuje perspektívu operátora aj dátového subjektu, keďže budú ovplyvnení v prípade, že dôjde k porušeniu údajov.

Stanovenie miery dopytu (nízka, stredná, vysoká) určuje výber kontrol súkromia z komplexného zoznamu kontrol súkromia, ktoré sú uvedené aj v smernici BSI PIA.

7.5 Súkromie zamerané na cieľ

Okrem prístupov založených na riziku k riešeniu súkromia, PRIPARE **Error! Reference source not found.** (projekt financovaný EÚ, ktorý vypracoval metodológiu súkromia) výslovne navrhuje **Error! Reference source not found.** dodržiavanie prístupu zameraného na cieľ pre uvedenie princípov súkromia na vysokej úrovni do prevádzky pre poskytnutie systému so základnou líniou, ktorá obsahuje základnú úroveň súkromia. Výraz „výslovne“ je podčiarknutý, pretože zatiaľ čo rámec BSI PIA popísaný v časti □ sa dá považovať (ako aj prístup založený na riziku) za zameraný na cieľ, nie je to tu výslovne uvedené. Tento prístup navrhnutý PRIPARE sa odporúča aj v nedávnej smernici CNIL PIA **Error! Reference source not found.**, kde identifikácia „Právnych kontrol“ dodržiava prístup zameraný na cieľ.

Prístup PRIPARE zameraný na cieľ dodržiava rovnaký postup ako smernice prístupnosti webového obsahu **Error! Reference source not found.** vypracované iniciatívou webovej prístupnosti prostredníctvom procesu W3C **Error! Reference source not found.**

Prístup zameraný na cieľ sa spolieha na tri základné kroky:

1. Identifikácia princípov súkromia, ktoré budú riadiť výber sústavy požiadaviek spojených so súkromím zadefinovaných interne alebo externe;
2. Stanovenie požadovanej úrovne zhody (PRIPARE navrhuje úrovne I, II a III) pre systém (toto rozhodnutie môže byť interne alebo externe obmedzené, teda právnym rámcom).
3. „Stanovenie použiteľnosti každej požiadavky súkromia v závislosti od špecifikácie systému, miery požadovanej a/alebo potrebnej zhody a iných organizačných obmedzení“

Prístup zameraný na cieľ je založený na existencii katalógu smerníc súkromia a požiadaviek, ktoré „sa musia stále vyvíjať a harmonizovať s komunitou zástancov súkromia“ **Error! Reference source not found.**, ktoré mapujú princípy vysokej úrovne podľa požiadaviek súkromia označených inou mierou zhody.

Je dôležité uviesť, že PRIPARE nepopisuje tento prístup ako samostatný prístup, ale ako rístup, ktorý bude súčasťou celkového prístupu systému a ktorý bude doplnený prístupom založeným na riziku.

7.6 Bezpečnosť

Zatiaľ čo sa táto analýza zameriava na súkromie a súkromie pomocou projektu, bezpečnosť je jedným z najvýznamnejších pilierov súkromia. Väčšina technológií podporujúcich súkromie alebo vylepšených riešení sa spolieha na bezpečnostné mechanizmy a vlastnosti pre dosiahnutie ich požadovanej miery súkromia. Napr. dôvernosc údajov sa dosahuje pomocou mechanizmov kódovania.

Preto musí súkromie dodržiavať holistický prístup zlučujúci koncepty súkromia a bezpečnosti a prístupy pre riešenie potrieb súkromia v rámci systému. V tomto zmysle existuje niekoľko iniciatív, nástrojov a metodológií, ktoré sa momentálne používajú v oblasti ICT, ktoré sa dajú vynútiť prístupmi PbD.

7.6.1 Cyklus životnosti rozvoja bezpečnosti u Microsoftu

Microsoft sa vo svojej metodológii spojenej s bezpečnosťou **Error! Reference source not found.** zameriava na jednu z medzier, ktorú nerieši žiadna z (už) uvedených iniciatív súkromia: „Pokrýva celý cyklus životnosti systému“.

Metodológia SDL sa spolieha na niekoľko postupov, ktoré by sa mali vziať do úvahy počas rôznych fáz cyklu životnosti systému.

Fáza	Postup
Školenie	1. Hlavné bezpečnostné školenie
Požiadavky	2. Stanovenie bezpečnostných požiadaviek
	3. Vytvorenie brán kvality / Bug Bars
	4. Vykonávanie hodnotení bezpečnosti a rizika súkromia
Projekt	5. Stanovenie projektových požiadaviek
	6. Vykonanie analýzy povrchu útoku / zníženia
	7. Modelovanie hrozieb používania
Implementácia	8. Používanie schválených nástrojov
	9. Odmietnutie nebezpečných funkcií

	10. Vykonanie statickej analýzy
Overenie	11. Vykonanie dynamickej analýzy
	12. Vykonanie čiastočného testovania
	13. Vykonanie revízie povrchu útokov
Vydanie	14. Vytvorenie plánu reakcie na incidenty
	15. Vykonanie revízie konečnej bezpečnosti
	16. Certifikácia vydania a archívu
Odpoveď	17. Vykonanie plánu reakcie na incidenty

Tabuľka 8: Fázy a postupy SDL Microsoftu

Druhým významným aspektom SDL Microsoftu je to, že poskytuje pomoc pri zlučovaní s technickými metodológiami, ktoré sú obvyčajne náročné v zmysle bezpečnosti, teda Scrum.

Zatiaľ čo všetky popísané postupy môžu ovplyvniť mieru súkromia systému zvýšením jeho bezpečnosti, mnohé z nich sa dajú „previesť“ do oblasti súkromia, čo by mohlo mať veľký vplyv na prístup PbD. Napr.:

- Modelovanie hrozieb: STRIDE **Error! Reference source not found.** vs LINDDUN **Error! Reference source not found.**
- Plán reakcie na incidenty: môže sa vzťahovať aj na incidenty súkromia
- Statická a dynamická analýza: môže sa vzťahovať aj na aspekty, napr. PiOS: Detekcia únikov súkromia v aplikáciách iOS **Error! Reference source not found.** alebo TaintDroid **Error! Reference source not found.**

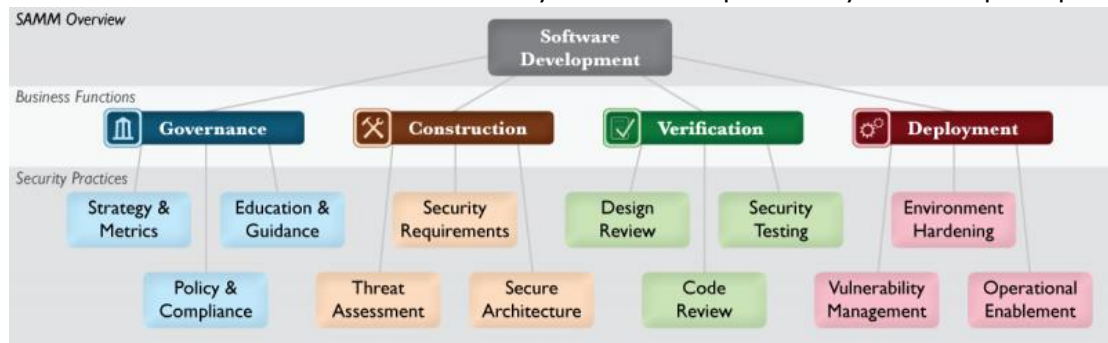
7.6.2 Otvorený projekt bezpečnosti webových aplikácií (OWASP)

„Otvorený projekt bezpečnosti webových aplikácií (OWASP) je celosvetovou neziskovou charitatívnou organizáciou, ktorá sa zameriava na zlepšenie bezpečnosti softvéru“ **Error! Reference source not found.** ustanovený v roku 2001.

Obsahuje veľké množstvo projektov (nástroje, knižnice, rámce, pravidelné správy, atď.), ktoré poskytujú softvérovým inžinierom, v rámci bezplatnej a otvorenej softvérovej licencie, materiál, ktorý môže pomôcť zlepšiť ich povedomie o bezpečnosti a v niektorých prípadoch dostávajú pomoc pre riešenie špecifických problémov. Niektoré vlajkové projekty OWASP, ktoré sú veľmi významné v oblasti bezpečnosti, predstavujú:

- **OWASP Top Ten:** Správa o bezpečnosti webových aplikácií, ktorá identifikuje 10 najkritickejších bezpečnostných rizík, podľa spoločnej zhody odborníkov. Pri každom z 10 najvyšších rizík poskytuje aj príklady zraniteľnosti, útoky a rady ako sa im vyhnúť.
- **OWASP Software Assurance Maturity Model (SAMM)** **Error! Reference source not found.:** otvorený rámec, ktorý pomáha organizáciám formulovať ich vlastnú stratégiu bezpečnosti softvéru. Je založený na troch úrovniach zrelosti pri

každom z 12 uvedených bezpečnostných postupov:



- **OWASP Application Security Verification Standard (ASVS)****Error! Reference source not found.**: zameriava sa na štandardizáciu rozsahu a úrovne prísnosti overovania bezpečnosti na trhu. Dá sa použiť ako:
 - Metrika na porovnanie miery dôvery webových aplikácií;
 - Pomoc pri bezpečnostných kontrolách;
 - Základ špecifikácie požiadaviek overenia bezpečnosti aplikácie.
- **OWASP Secure Coding Practices Quick Reference Guide****Error! Reference source not found.**: poskytuje sústavu postupov bezpečnostného kódovania, ktorá pomáha zmierniť najbežnejšie zraniteľnosti softvéru.
- **OWASP Security Principles****Error! Reference source not found.**: Cieľom tohto projektu je identifikovať a popísať minimálnu funkčnú sústavu princípov, ktoré musia byť prítomné v bezpečnom projekte;
- **OWASP Risk Rating Methodology****Error! Reference source not found.**: súčasť OWASP Testing Guide Project**Error! Reference source not found.**, je založená na šiestich krokoch, ktoré pomáhajú hodnotiť bezpečnostné riziká a zohľadňuje široký rozsah faktorov pre odhad vplyvu a pravdepodobnosti rizík (teda skúsená úroveň, motív a príležitosť agentov hrozieb v zmysle pravdepodobnosti a financií, poškodenia reputácie, nezhody a množstva osobných údajov, ktoré sa dajú šíriť na odhadnutie vplyvu).



Obrázok 9: Kroky metodológie hodnotenia rizík OWASP

7.6.3 Ostatné veľké bezpečnostné iniciatívy

Okrem noriem uvedených v tejto časti sa tu nachádza mnoho dostupných bezpečnostných noriem a projektových bezpečnostných noriem, prístupov a smerníc, v závislosti od domény, technológie a iných charakteristík systému a organizácie. Napr.:

- ISO/IEC 27001:2013 Informačné technológie — Bezpečnostné techniky — Systémy riadenia bezpečnosti informácií — Požiadavky **Error! Reference source not found.**
- ISO/IEC 27002:2013 Informačné technológie — Bezpečnostné techniky — Zákoník postupov pre kontroly bezpečnosti informácií **Error! Reference source not found.**
- COBIT ISACA 5 **Error! Reference source not found.**
- Bezpečnostná norma priymseelných údajov platobnej karty **Error! Reference source not found.**
- Najlepšie postupy Android pre bezpečnosť a súkromie **Error! Reference source not found.**
- Bezpečnostná príručka iOS **Error! Reference source not found.**
- Bezpečnostná príručka Red Hat Enterprise Linux 6 **Error! Reference source not found.**
- Smernice bezpečného vývoja smartphonov ENISA pre vývojárov aplikácií **Error! Reference source not found.**
- Matrica kontroly cloudu bezpečnostnej aliancie cloudu **Error! Reference source not found.**

7.7 Normy súkromia a orgány

Okrem bezpečnostných noriem uvedených v časti 0 a iných noriem súkromia, ktoré tu už boli uvedené (napr. OASIS PMRM a NIST PRMF) sú tu aj iné normy (zverejnené a vo vývoji), ktoré sa pokúšajú poskytnúť spoločný pohľad na to, čo je to súkromie a ako by sa malo spracovávať v oblasti ICT:

- ISO/IEC 29100:2011 Informačné technológie -- Bezpečnostné techniky -- Súkromný rámec **Error! Reference source not found.**
- ISO/IEC 29101:2013 Informačné technológie -- Bezpečnostné techniky -- Súkromný rámec architektúry **Error! Reference source not found.**
- ISO/IEC CD 29134 -- Hodnotenie vplyvu súkromia – Metodológia [62]
- [63]
- Rámec súkromia MITRE [64]

Okrem noriem súkromia, ktoré sa práve vypracovávajú, sú tu niektoré organizácie na úrovni EÚ alebo entity, ktoré poskytujú pomoc pri ochrane osobných údajov a sú veľmi relevantné:

- „Článok 29 Pracovná strana ochrany údajov bol ustanovený v rámci smernice 95/46/EC Európskeho parlamentu a Rady z 24. októbra 1995 o ochrane osôb s ohľadom na spracovávanie osobných údajov a o voľnom pohybe takýchto údajov“ **Error! Reference source not found.** Článok 29 pravidelne vydáva nezáväzné stanoviská, pracovné dokumenty a listy s cieľom poskytnúť rady v záležitostiach spojených so súkromím. Stanoviská článku 29 zahŕňajú a pomohli tvarovať aktuálne prístupy súkromia. Niektoré najvýznamnejšie dokumenty alebo stanoviská pre túto správu sú nasledovné:
 - Stanovisko 03/2014 o oznamovaní porušenia osobných údajov **Error! Reference source not found.**

- Stanovisko 8/2014 o nedávnom vývoji v oblasti Internet of Things **Error! Reference source not found.**
 - Pracovný dokument 02/2013, ktorý poskytuje rady k dosiahnutiu súhlasu s cookies **Error! Reference source not found.**
 - Stanovisko 05/2014 Techniky anonymizácie **Error! Reference source not found.**
 - Prehlásenie o úlohe prístupu založeného na riziku v právnych rámcoch ochrany údajov **Error! Reference source not found.**
- Agentúra Európskej únie pre bezpečnosť sietí a informácií (ENISA) pracuje pre inštitúciu EÚ a predstavuje reakciu EÚ na kybernetickú bezpečnosť a otázky súkromia v rámci Európskej únie. Najvýznamnejšie publikácie spojené s bezpečnosťou sú:
 - Súkromie a ochrana údajov v projekte – od politiky k technológii **Error! Reference source not found.**
 - Príručka ENISA k tomu, ako zvýšiť povedomie o bezpečnosti informácií **Error! Reference source not found.**

7.8 Súkromie softvéru verzus hardvéru

Až doteraz sa táto kapitola zameriavala na metodologické prístupy k riešeniu súkromia na organizačnej úrovni a na to ako sa integrujú s procesom budujúcim systém. nasledujúce dve podriadené časti prejednávajú špecifické opatrenia a prístupy pre podporu súkromia na úrovni systému.

Hlavný rozdiel sa urobí medzi opatreniami súkromia „softvéru“ a opatreniami súkromia „hardvéru“. Prvé opatrenia obsahujú všetky tie opatrenia, kontroly a prístupy, ktoré si stále vyžadujú istú dôveru minimálne v tretiu stranu. Dátové subjekty musia dôverovať, že kontrolór a spracovávateľ údajov budú dodržiavať správne zadanú politiku súkromia. Na druhej strane konečným cieľom opatrení súkromia hardvéru je minimalizovať túto potrebu dôvery (napr. kódovať údaje pred odoslaním do cloudu. Zatiaľ čo časť 0 sa zameriava na prístupy súkromia softvéru, časť 0 uvádza zoznam technológií podporujúcich súkromie, ktoré sa dajú považovať za hardvérové.

7.9 Technológie podpory súkromia softvéru

Na trhu a vo výskume je už viacero nástrojov a funkcií, ktorých cieľom je poskytnúť používateľovi väčšiu kontrolu nad jeho údajmi, podľa základných princípov PbD v zmysle „Viditeľnosti a transparentnosti - Udržujte ich otvorené“ a „Dodržiavanie súkromia používateľa - Udržujte ich zamerané na používateľa“.

7.9.1 Technológie podpory transparentnosti (TET)

Existuje široký rozsah dostupných TET a ich funkcie, výhody a nevýhody sa môžu líšiť. Tu je uvedený zoznam niektorých príkladov týchto technológií:

- **Ikony súkromia:** ich cieľom je poskytnúť vizuálne znázornenie a zjednodušenie najvýznamnejších informácií o súkromí, ktoré sa obyčajne poskytujú prostredníctvom nešikovnej politiky súkromia. Tento prístup, ktorý je súčasťou

návrhu Európskeho parlamentu všeobecného nariadenia o ochrane údajov **Error! Reference source not found.**, už má isté implementácie

- Mozilla Privacy Icons **Error! Reference source not found.**
- Disconnect.me Icons **Error! Reference source not found.**
- **Panely súkromia:** obyčajne informujú používateľov o ich uložených osobných údajoch a o tom ako sa používajú. Zároveň môžu fungovať ako centrálny systém riadenia súkromia, kedy dátové subjekty dokážu poskytnúť a odvolať súhlas k prístupu a spracovaniu údajov. Je dôležité zdôrazniť, že toto opatrenie môže byť zavádzajúce, ak automaticky nezhrádza a neprotokoluje všetky príslušné údaje o subjekte. Medzi niektoré príklady, ktoré prichádzajú do úvahy, patria
 - Google Privacy Dashboard **Error! Reference source not found.**
 - W3C Privacy dashboard (založený na PrimeLife privacy dashboard) **Error! Reference source not found.**
- **Nástroje používateľa:** tieto nástroje nezávisia od poskytovanej služby, v rámci ktorej sa zverejňujú osobné údaje subjektu, ale riadi informácie spojené s takýmto poskytovaním prostredníctvom aplikácie alebo pluginov:
 - PrivOwney **Error! Reference source not found.:** doplnok prehliadača, ktorý umožňuje dátovým subjektom „bezpečne a selektívne získavať informácie, ktoré sa denne ukladajú na webových stránkach, pridávať ich a ukladať do databázy osobných informácií.
 - PrimeLife Data Track **Error! Reference source not found.**
- **Spojené s povedomím:** používajú sa na to, aby sa dátovým subjektom prezentovali riziká súkromia, ktorým sú vystavení, podľa ich osobného využívania nástrojov, služieb a zariadení:
 - Lightbeam: doplnok prehliadača, ktorý ukazuje používateľom ako môžu sledovať špecializovanú službu v rámci používateľov v rôznych a zjavne nesúvisiacich službách **Error! Reference source not found.**
 - ToS; DR: aktívny projekt, ktorý pomáha používateľom pochopiť a sledovať zmeny podmienok a politiky súkromia webových stránok. **Error! Reference source not found.**
 - Panopticlick: sledovanie služieb môže vynútiť jednoznačnosť konfigurácie každého webového prehliadača pre sledovanie používateľov v rámci rôznych služieb. Panopticlick pomáha používateľom pochopiť, aký „jedinečný“ je ich profil prehliadača. **Error! Reference source not found.**
 - Povolenia F-Secure App **Error! Reference source not found.:** aplikácia pre Android poskytuje používateľom „veľmi jednoduchý a užitočný pohľad na všetky nainštalované aplikácie, jednoduchú identifikáciu nechcených aplikácií, ktoré môžu ohroziť ich súkromné informácie“

Hlavné problémy alebo medzery, ktoré sa budú riešiť v rámci týchto technológií, sú

- Poskytovatelia služieb, ktorí poskytujú svoje vlastné TETs, nemusia poskytovať skutočne celkový pohľad na ich údaje a na účel, na ktorý sa používajú, za účelom ochrany záujmov poskytovateľa. Používatelia si nemusia byť vedomí tejto čiastočnej transparentnosti a majú falošný pocit „kontroly“;
- Neposkytujú pohľad na to, ako sa údaje spracovávajú alebo ktoré algoritmy sa používajú na jeho proces.

7.9.2 Nástroje preferencie súkromia

Zatiaľ čo predchádzajúci zoznam nástrojov (časť 0) sa zameriava na nástroje, ktoré „ukazujú“ používateľom, aké sú ich riziká súkromia, nástroje preferencie súkromia umožňujú používateľom vykonávať istú kontrolu nad ich údajmi, vyjadrením ich preferencie súkromia pomocou technologických prostriedkov a používania automatických vynucovacích mechanizmov.

V roku 2000 sa navrhol celkový rámec preferencií súkromia (P3P **Error! Reference source not found.**). Nedostatočná jasnosť, zavádzajúca prezentácia politiky súkromia a iné problémy však obmedzili jeho prijatie. Na rozdiel od rámcov všeobecnej úrovne majú poskytovatelia služieb tendenciu poskytovať svojim používateľom viac zameraný rámec (napr. sociálne siete a možnosti konfigurácie nastavenia viditeľnosti publikácií: verejnosť, priatelia, práca, rodina...).

V každom prípade je zadefinovanie a navrhnutie efektívneho UI pre kontrolu súkromia pochopiteľného pre používateľov srôzneho vekového rozsahu alebo rôznej kultúry náročnou alebo skôr komplexnou úlohou.

Medzi ostatné príklady týchto nástrojov preferencie súkromia patria blokovacie reklamy **Error! Reference source not found.** (aktuálne populárne vďaka funkcii blokovania reklamy iOS 9 od Apple) alebo špecifikácia nesledovania **Error! Reference source not found.**, ktorá umožňuje používateľom vyjadriť svoje preferencie ohľadom prijateľnej reklamy alebo postupov sledovania. Opäť, ako pri nástrojoch TETs, si to vyžaduje istú dôveru k tretej strane (teda poskytovateľovi služby, ktorý reklamu blokuje) alebo priamo k poskytovateľovi služby, pričom dúfame, že budú vynucovať preferencie používateľov a ich politiku súkromia.

A neposlednom rade ide o preferencie súkromia poskytované poskytovateľmi služby, ktorých cieľom je chrániť súkromie dátových subjektov pred ostatnými účastníkmi, výnimočne chrániť súkromie pred samotným poskytovateľom služby.

7.10 Technológie podpory súkromia hardvéru

Nižšie je uvedený zoznam technológií podporujúcich súkromie a prístupov, ktorých hlavným cieľom je minimalizovať úroveň dôvery, ktorú musia dátové subjekty vložiť do kontrolóra údajov, spracovávateľa alebo tretej strany

7.10.1 Riadenie prístupu k identite

Riadenie prístupu k identite je kľúčovým aspektom súkromia, keďže obsahuje prostriedky na zaistenie toho, aby subjekt, ktorý sa dostal k istým osobným údajom, je ten, za koho sa vydáva a aby bol oprávnený (podľa vopred stanovených politík) pristupovať k takýmto údajom. Aj napriek tomu, že je potrebné chrániť si súkromie, IAM sú takisto náročné z pohľadu súkromia, keďže v prípade, že sa správne neimplementujú, môžu umožniť poskytovateľom služieb alebo tretím stranám sledovať používateľov alebo vytvárať ich profily spomedzi všetkých ostatných služieb, ku ktorým sa pristupuje v rámci rovnakej identity.

Medzi príklady najnovších protokolov a nástrojov IAM s funkciami súkromia patria:

- **Anonymné systémy prihlasovacích údajov** ako je Idemix **Error! Reference source not found.** alebo U-Prove **Error! Reference source not found.**, algoritmy určené na ochranu súkromia a identity. Umožňujú teda preukázať, že je osoba v danom vekovom rozsahu bez uvedenia dátumu narodenia;
- **Autentifikačné protokoly** ako je Just Fast Keying (JKF) **Error! Reference source not found.**, ktorý umožňuje otvoriť bezpečné relácie medzi dvomi stranami, pri overení ich údajných identít a dosiahnutí dokonalého utajenia. Tento protokol využíva HTTPS takým spôsobom, že aj v prípade, že sa údajné identity overia, môže chrániť identitu niektorých strán;
- **Spojené systémy riadenia** sú založené na spolupráci samostatných entít pri autentifikácii používateľov a preposlaní ich identity špecifickému poskytovateľovi služby. Zatiaľ čo sa tu nachádza mnoho systémov jednoduchého prihlasovania na základe tohto prístupu (napr. Facebook, Google), ktoré majú minimálne funkcie súkromia a umožňujú silné sledovanie alebo vytváranie profilov používateľov, nachádzajú sa tu aj systémy s pokročilejšími funkciami súkromia. Teda STORK **Error! Reference source not found.**, Shibboleth **Error! Reference source not found.** a iné umožňujú selektívne šírenie atribútov, ktoré pomáhajú chrániť sa pred poskytovateľmi tretích strán, ale neodstraňujú potrebu dôvery v identitu poskytovateľa.
- **Prihlasovacie údaje založené na atribútoch**, na rozdiel od anonymných systémov prihlasovacích údajov, ktoré tu už boli uvedené, dávajú do centra všetkých transakcií identity používateľa a nemusia sa spoliehať na žiadneho poskytovateľa identity. ABC4Trust **Error! Reference source not found.** je projekt financovaný EÚ, ktorý poskytuje implementáciu referencie tohto prístupu.

7.10.2 Úroveň komunikácie

Internet nebol vytvorený s ohľadom na bezpečnosť alebo súkromie. Fyzické siete poskytujú obmedzené záruky ohľadom dôvernosti komunikácie. Bezdrôtová komunikácia je ešte náročnejšia, a aj napriek tomu používaná bezpečnostná norma nedokáže zabrániť sledovaniu. Ochrana komunikácie medzi dvomi stranami je dvojakým prvkom. Na jednej strane sa musí prevádzaný kontext ochrániť, aby sa zabránilo neželanému šíreniu osobných údajov. Na druhej strane komunikačné metadáta, ktoré obsahujú príslušné strany, časy a dĺžky komunikácie a množstvo prenášaných údajov umožňujú strane, ktorá vykonáva tajné odpočúvanie, vytvárať vzorce prehliadania, profily, vzorce využívania služieb, atď. Existujú rôzne metódy a nástroje, ktoré spracovávajú jeden z týchto aspektov alebo oba aspekty:

- **Randomizácia MAC adresy**: na spracovávanie metód sledovania na základe Wi-Fi MAC zariadení, ktoré jedinečne identifikujú zariadenia s povolenou sieťou Wi-Fi (dostupné v iOS **Error! Reference source not found.** a Windows 8)
- **Kódovanie služby klientov**: TLS (Transport Layer Security), SSH (Secure Shell) alebo IPSec (Internet Protocol Security) sú rozšírené príklady ochrany komunikácie pomocou „infraštruktúry verejného kľúča“. Tieto prístupy nedokážu chrániť komunikačné metadáta.
- **Koncové kódovanie**: vždy, keď komunikujú dve strany cez poskytovateľa služby tretej strany, kódovanie služby klientov medzi stranami a poskytovateľom služby

vyvoláva hlavné otázky súkromia (poskytovateľ služby by mohol tajne odpočúvať prenášaný obsah). Koncové protokoly kódovania, kde sa môžu k obsahu prenosu dostať len obe strany, boli navrhnuté pre služby ako je email**Error! Reference source not found.**, komunikácia VoIP**Error! Reference source not found.**, okamžité správy**Error! Reference source not found.**. Tento typ kódovania sa zameriava na ochranu obsahu komunikácie

- **Anonymná komunikácia:** zameriava sa na ochranu komunikačných metadát (napr. skrývanie identity/miesta odosielateľov správ a prijímateľov od nich alebo od tretích strán):
 - **Virtuálne súkromné siete (VPNs):** pohyb používateľov je kódovaný a odosiela sa do brány, cez ktorú sa dostáva do otvoreného Internetu. Nepriateľské sledovanie klienta nemôže vyvodíť cieľovú destináciu prenosu. Používatelia musia dôverovať poskytovateľovi VPN, keďže vedie VŠETKY ich prenosy.
 - **Onion routing:** spočíva na viacerých uzloch, cez ktoré sa prenáša správa. Každý uzol pozná len predchádzajúci a nasledujúci uzol, kam má správa ísť. Protivník by musel kontrolovať veľký počet týchto uzlov, aby dokázal efektívne sledovať aktivity používateľa
 - **Zmiešané siete:** Podporuje prístup onion-routing nastavením jednotnej veľkosti správy a umožnením pokrytia potenciálnej štatistickej analýzy omeškaním správy**Error! Reference source not found.**;
- **Steganografické techniky:** zatiaľ čo sa kryptografia zameriava na skrývanie obsahu správy, steganografia sa zameriava na skrývanie existencie takejto správy jej moduláciou tak, aby vyzerala ako krycia správa. Príkladom je SkypeMorth**Error! Reference source not found.**, inteligentný systém, ktorý mení prenosy Tor na video prenosy Skype.

7.10.3 Úroveň ukladania

Cieľom súkromia na úrovni ukladania je zabrániť prístupu neželaných strán k osobným údajom uloženým v systéme. V závislosti od príslušného modelu hrozby (napr. keď je poskytovateľ služby ukladania dôveryhodný alebo nie), nespojitosti ochrany údajov (napr. kódovanie celého systému súborov verzus individuálnych atribútov dátového subjektu) a požiadaviek kontroly prístupu je dostupných mnoho kontrol ukladania a prístupu k údajom:

- **Lokálne ukladanie kódovania:** kódovanie celej podpory ukladania (HDD alebo vymeniteľná jednotka) alebo len obsah súborov a nie metadáta predstavujú veľmi rozsiahly prístup prítomný v mnohých systémoch:
 - Funkcie kódovania celého disku Android**Error! Reference source not found.** a iOS**Error! Reference source not found.**
 - FileVault**Error! Reference source not found.** prítomný v Mac OS X od verzie 10.3 v najnovšej verzii kóduje celý spúšťač objemu OS X.
 - TrueCrypt**Error! Reference source not found.** (prerušený a nedávno odhalený ako zraniteľný) a BitLocker**Error! Reference source not found.** kóduje celé jednotky operačného systému, sekundárne jednotky a dokonca vymeniteľné zariadenia vo Windows OS. Linux Unified Key Setup

(LUKSError! Reference source not found.) používa rovnaký prístup, ale pre distribúciu Linux.

- **Bezpečné vzdialené ukladanie:** dnes sa dostávajú do popredia vďaka vpádu cloud computing a nenákladného ukladania na cloud služby ukladania na cloud (teda Dropbox má viac ako 50 miliónov zaregistrovaných používateľov a viac ako 500 miliónov súborov ukladaných denne). Aj napriek tomu, že tieto služby lódujú súbory pomocou najnovších kódovacích algoritmov, pokiaľ je toto kódovanie založené na kľúčoch, ktoré nie sú plne kontrolované dátovým subjektom, tento systém neposkytuje súkromie pred poskytovateľom služby. Jedným riešením je to, aby používatelia svoje citlivé údaje pred načítaním na cloudError! Reference source not found. zakódovali, ale toto je spojené s pokutou za stratu funkčnosti na strane servera (napr. serverový výskum), keďže server nemôže tieto údaje vidieť. Týmto obmedzeniam sa dá vyhnúť pomocou výpočtov zachovávajúcich súkromie, ako je homomorfné kódovanie (pozrite si časť □□), ktoré umožňuje počítanie niektorých operácií v kódovaných údajoch.
- **Ukladanie do databázy:** ide o veľmi širokú oblasť, keďže obsahuje viacero prístupov, pohľadov a modelov hrozieb, ktoré sa použijú na ochranu osobných údajov. Pokiaľ ide o tento pohľad, zatiaľ čo sú zjavné prípady, kedy sa musia záznamy osobných údajov uložených v databázach chrániť, existujú ďalšie nie až tak zjavné prípady, kedy sa musí chrániť aj súkromie dotazov v databáze, aby sa zabránilo vytváraniu profilov používateľov. Niektoré z najbežnejších metód ochrany dátových záznamov sú popísané v tejto časti. Je dôležité uviesť, že tieto mechanizmy sa dajú použiť pred uložením údajov, pred ich zverejnením a počas dotazu v databáze pri dotazovaných údajoch alebo v ich výsledkoch.
 - *Dodatočný hluč:* dodržiavanie istej štatistickej distribúcie, ktorá výrazne neovplyvňuje globálne parametre údajov (priemerná, štandardná odchýlka...).
 - *Mikro spájanie:* jednotlivé záznamy „sa pred zverejnením zoskupia do malých sústav. Každá sústava by mala obsahovať minimálne vektory údajov k , aby sa zabránilo šíreniu jednotlivých informácií, kde k predstavuje hodnotu konštanty prednastavenú chráničom údajov“Error! Reference source not found.
 - *Prepínanie atribútov* medzi záznamami, udržiavanie celkových štatistických opatrení
 - *Post-randomizácia*Error! Reference source not found.: pri každom zázname v dátovom súbore, podľa stanoveného mechanizmu pravdepodobnosti sa zmení kategória premennej. Keďže je tento mechanizmus pravdepodobnosti známy, charakteristiky latentných pravdivých údajov môžu objektívne predstavovať narušené údaje.
 - *Odber vzoriek:* namiesto zverejnenia celého dátového súboru zverejnite len jeho vzorku.
 - *Generalizácia:* súvislé atribúty sa zmenia na sústavu kategórií a kategorických atribútov, ktoré sa zoskupia do novej sústavy kategórie.
 - *Generovanie údajov:* generovanie náhodných vzoriek (podľa vopred zadefinovaného štatistického modelu) údajov, neodlíšiteľné od skutočných údajov sa generujú a zmiešajú s pôvodnými údajmi

- *Obmedzenia dotazov*: v niektorých prípadoch môžu databázy chrániť osobné údaje zablokovaním jednotlivých dotazov alebo reťazcov dotazov, ktoré môžu odhaliť alebo viesť k odhaleniu osobných údajov
- *Metrika súkromia* je určená na meranie rizika opätovnej identifikácie alebo šírenia atribútov v sústavách údajov. Táto metrika môže slúžiť na porovnanie situácií a-priori a a-posteriori pre zmeranie efektívnosti procesu anonymizácie alebo na porovnanie rôznych metód anonymizácie. V literatúre sú popísané tri hlavné metriky súkromia:
 - Anonymita k**Error! Reference source not found.**: sústava údajov má vlastnosť anonymity k vtedy, ak sa každá osoba nedá odlíšiť minimálne od ostatných osôb k-1, ktoré sú prítomné v rovnakej sústave údajov.
 - Diverzita L**Error! Reference source not found.**: rozširuje definíciu anonymity k a pridáva diverzitu v rámci skupiny pri citlivých hodnotách v mechanizme anonymizácie.
 - Blízkosť T**Error! Reference source not found.**: rozširuje model diverzity I odlišným posudzovaním hodnôt atribútu zohľadnením distribúcie každého dôverného atribútu v skupine
- *Prístup k databáze* (Získanie súkromných informácií): cieľom týchto technológií je chrániť používateľov, ktorí prístupujú k vyhľadávateľom alebo databázam od svojich poskytovateľov a vlastníkov. Používateľ môže zadať dotaz do databázy alebo vyhľadávača bez zistenia, ktorý dotaz sa vykonáva alebo ktoré údaje sa získavajú. Navrhli alebo dodržujú sa viaceré postupy:
 - Jedna strana: používatelia posielajú falošné dotazy, aby databáza alebo poskytovateľ služby hľadania nezistil, ktorá správa je tá pôvodná (napr. TrackMeNot**Error! Reference source not found.**)
 - Peer-to-peer: používateľ môže odosielať dotazy, ktoré pochádzajú od partnerov a naopak;
 - Onion-routing: ako napríklad JonDonym**Error! Reference source not found.** a dodržiavanie schémy popísanej v časti □.
 - Na báze proxy: používateľ pošle dotazy do proxy, ktorý zodpovedá za odosielanie a vrátenie výsledkov dotazov z cieľovej služby (napr. DuckDuckGo**Error! Reference source not found.**). Týmto prístupom sa neodstráni potreba dôvery, ale presunie sa od poskytovateľa služby na poskytovateľa proxy.

7.10.4 Úroveň počítania

Zatiaľ čo sa minimálne riešilo súkromie a bezpečnosť na úrovni prenosu a ukladania, cloud computation priniesol novú sústavu výziev, ktoré bránia organizácii s' dešifrovať jej výpočtové úlohy bez narušenia bezpečnosti a súkromia ich údajov.

Výpočty chrániace súkromie predstavujú sústavu technológií, metód a prístupov, ktoré umožňujú jednej alebo viacerým stranám vyrábať funkciu na sústave vstupov, pri zachovaní súkromia vstupov a výstupov pre strany výpočtu. Existujú dva hlavné prístupy:

- Homomorfne kódovanie **Error! Reference source not found.**: forma kódovania, ktoré umožňuje vykonávať malú sústavu operácií v kódovanej oblasti za predpokladu, že kódovaný výsledok sa zhoduje s kódovaným výsledkom tej istej operácie vykonanej na nekódovaných údajoch;
- Bezpečný výpočet viacerých strán **Error! Reference source not found.** (MPC): umožňuje viacerým stranám spoločne vypočítať funkciu pri zachovaní súkromia vstupov. Obyčajne sa tu nachádza jeden súkromný výstup pre každú stranu;

Oba prístupy sú praktické len pre niektoré kategórie jednoduchých scenárov, ale dajú sa vynútiť, aby automaticky zaviedli bezpečnosť a súkromie v systéme. Tieto prístupy boli navrhnuté na riešenie problémov súkromia v scenároch ako je e-Voting **Error! Reference source not found.**, meranie spotreby smart grid **Error! Reference source not found.** alebo spolupráca v oblasti lekárskeho výskumu **Error! Reference source not found.**.

7.11 Architektonické prístupy

Táto správa už pokryla postupy spojené so súkromím pre vylúčenie požiadaviek súkromia (napr. časti 7.2, 7.3.1, 0 alebo 0). Presun z požiadaviek súkromia koncových používateľov na systémový projekt je veľmi náročným aspektom súkromia.

Systémy obyčajne nie sú vytvorené ako celok, ale ako komplexná sieť jednotlivých komponentov, ktoré interagujú s rôznymi vrstvami, každá vo vlastnom celi súkromia, ktorý sa musí kombinovať. Súkromie v systéme nie je len také slabé ako jeho najslabší komponent, existuje ak prípad, kedy komponenty s vlastnosťami dodržiavania súkromia v kombinácii vedú k zníženiu vlastností súkromia týchto individuálnych komponentov, a tým aj celého systému. Existuje tu niekoľko návrhov toho, ako začať riešiť architektonické aspekty súkromia v priebehu projektu systému.

7.11.1 Architektúry podporujúce súkromie

ENISA **Error! Reference source not found.** obsahuje návrh Antonia Kunga **Error! Reference source not found.** použiť podobný prístup ako sú prístupy vypracované v inštitúte Carnegie Mellon Software Engineering Institute (metóda analýzy nákladov a ziskov - CBAM **Error! Reference source not found.** a metóda analýzy porovnania architektúry – ATAM **Error! Reference source not found.**). Výsledný návrh predstavuje reťazový proces obsahujúci nasledujúce kroky:

1. Predloženie úvodnej architektúry.
2. Identifikácia a prioritizácia scenárov a atribútov kvality.
3. Identifikácia potenciálnej architektonickej bezpečnosti a vylepšení súkromia.
4. Výber a použitie architektonických postupov súkromia a bezpečnosti pre scenár.

Proces PEAR sa spolieha na výber a používanie (na architektonickej úrovni) rôznych prístupov súkromia, ktoré môžu zahŕňať PETs (časť 0), stratégie súkromia (časť 0) a vzorce súkromia (časť 7.11.2), ktoré predstavujú spojené koncepty.

7.11.2 Vzorce súkromia

Vo všeobecnosti sa dá vzorec považovať za opätovne použiteľné riešenie bežne sa vyskytujúceho problému. Vo vývoji softvéru vzorce dizajnu popisujú „bežne sa opakujúcu štruktúru komunikačných komponentov, ktorá rieši všeobecný problém dizajnu v príslušnom kontexte“**Error! Reference source not found.** Tento prístup umožňuje projektantom systému zamerať sa na systematický rozklad systému a vybrať si správny vzorec, ktorý už poskytne istú záruku ohľadom efektívnosti.

PRIPARE**Error! Reference source not found.** Projekt financovaný EÚ vytvoril sústavu vzorcov súkromia na úrovni EÚ**Error! Reference source not found.**, ktorá už obsahuje niektoré z týchto opätovne použiteľných riešení, ktoré dokážu pomôcť riešiť opakujúce sa problémy súkromia systému.

7.11.3 *Stratégie projektu súkromia*

Zatiaľ čo projektové vzorce môžu byť veľmi konkrétne a môžu riešiť veľmi špecifické problémy, projektové stratégie sú na vyššej úrovni abstrakcie a popisujú všeobecný prístup k dosahovaniu špecifických cieľov projektu. V prípade súkromnej domény stratégie projektu súkromia špecificky riešia ciele súkromia. Jaap-Henk Hoepman identifikoval a charakterizoval osem stratégií projektu súkromia**Error! Reference source not found.**, ktoré riešia princípy súkromia ISO 29100:

- **Minimalizovať:** Množstvo osobných údajov, ktoré sa spracovávajú, by malo byť obmedzené na minimálne možné množstvo;
- **Skryť:** Všetky osobné údaje a ich vzájomné vzťahy, by sa mali skryť pred jednoduchým pohľadom
- **Oddeliť:** Osobné údaje by sa mali spracovávať na základe distrúcie, v samostatných priestoroch, ak je to možné
- **Spojiť:** Osobné údaje by sa mali spracovávať na najvyššej miere spájania a s najmenšími možnými podrobnosťami, pri ktorých sú (ešte) užitočné
- **Informovať:** Dátové subjekty by mali byť vhodne informované pri každom spracovávaní osobných údajov
- **Kontrolovať:** Dátové subjekty by mali mať k dispozícii agentúru na spracovávanie ich osobných údajov.
- **Vynútiť:** Mala by sa zaviesť a vynucovať politika súkromia kompatibilná s právnymi požiadavkami
- **Preukázať:** Musíte byť schopný preukázať zhodu s politikou súkromia a so všetkými platnými právnymi požiadavkami

7.12 Holistický prístup

Zatiaľ čo každý z prístupov uvedených v tejto správe môže byť užitočný samostatne, zdá sa, že medzi nimi neexistuje dostatočné prepojenie. Je teda potrebné poskytnúť holistický rámec, ktorý obsahuje všetky tieto postupy, a navrhnúť, ako by sa dali skombinovať pre maximalizáciu ich efektívnosti.

PRIPARE vypracoval metodologický prístup**Error! Reference source not found.** založený na „najlepšom type“ spomedzi mnohých uvedených prístupov, ktorý je:

- ľahko pochopiteľný a ľahko použiteľný,

- založený na princípoch,
- poskytovaný s normami hodnotenia rizika,
- navrhnutý tak, aby pokryl celý cyklus životnosti systému,
- flexibilný, aby sa dokázal prispôbiť v závislosti od podstaty projektu a získavaných informácií,
- užitočný pre rôznych účastníkov,
- zapojený do technologických postupov.

Metodológia PRIPARE sa spája s referenčným modelom PMRM s konceptmi z bezpečnosti na základe projektu, PIAs, prístupmi zameranými na cieľ a architektonickými postupmi pre poskytnutie vlastného referenčného modelu. Pri tomto modeli PRIPARE navrhuje reťazovú metodológiu založenú na procese pre doplnenie existujúcich organizačných postupov a metodológií, aby historicky pokryli aspekty súkromia systému:

Environment & Infrastructure						
• Organizational Privacy Architecture • Promote privacy awareness						
Analysis	Design	Implementation	Verification	Release	Maintenance	Decommission
• Preliminary actions • Functional Description and High-Level Privacy Analysis • Privacy requirements operationalization • Detailed Privacy Analysis • Risk management • Legal compliance	• Top-down architecture design • Bottom-up architecture design • Privacy Enhancing Architecture (PEAR) design • Privacy Enhancing Detailed Design • User-centered UI design	• Privacy implementation	• Security & Privacy dynamic analysis • Security & Privacy static analysis • Accountability	• Create Incident Response Plan • Create system decommissioning plan • Final Security & Privacy review • Publish PIA report	• Execute incident response plan • Security & Privacy verifications	• Execute decommissioning plan

Zatiaľ čo PRIPARE už zverejnil svoju prvú verziu metodológie, druhá a vylepšená verzia sa očakáva krátko po ukončení projektu (október 2015).

8 Odporúčaná metodológia PbD pri riadení projektu systému bezpečnosti ICT

Prostredníctvom hodnotenia spoločných bodov prístupov PbD podľa analýzy v kapitole 7 vyššie, ako aj zohľadnenia identifikovaných medzier táto časť uvedie odporúčania metodológie pre riadenie PbD v rámci projektu systému bezpečnosti ICT pri ochrane osobných údajov.

Vybudovanie štruktúry súkromia na organizačnej úrovni

Súkromie podľa projektu a postupy budovania súkromia sa musia podporovať na organizačnej úrovni. Podľa veľkosti organizácie by sa mala vybudovať kancelária pre ochranu súkromia a mala by obsahovať minimálne právnych odborníkov a odborníkov na súkromie v oblasti/iach, na ktoré sa vzťahuje vypracovávaný systém ICT.

Táto kancelária pre ochranu súkromia bude zodpovedná za vývoj politiky súkromia, ktorá riadi systémy ICT spojené so systémom vzdelávania a za identifikáciu a budovanie vhodných inventárov osobných údajov spojených so vzdelávaním, rizík súkromia, PETs, vzorcov súkromia, kontrol súkromia. Medzi ostatné úlohy, za ktoré by mala táto štruktúra zodpovedať, patria:

- Vypracovanie významnej metriky súkromia pre zmeranie a porovnanie ich vlastnej zrelosti súkromia a úrovni súkromia existujúcich a nových systémov ICT;
- Riešenie problémov spojených so súkromím v rôznych projektoch;
- Vypracovanie základnej línie požiadaviek súkromia, ktoré musia všetky nové systémy ICT obsahovať a používať na príslušné procesy;
- Vytvorenie kampaní na zvyšovanie povedomia o otázkach súkromia zameraných na všetkých účastníkov systému ICT;

Medzi referencie, ktoré sú relevantné pre toto odporúčanie, patria:

- UK ICO obsahuje Prílohu (4) vo svojej príručke **PIA****Error! Reference source not found.**, ktorá hovorí o stratégiách súkromia a o tom, ako sa v nich pozitívne odrážajú organizačné prístupy k súkromiu;
- Príručka ENISA k tomu, ako zvýšiť povedomie o bezpečnosti informácií**Error! Reference source not found.**;
- Súbor vzorov súkromia PRIPARE**Error! Reference source not found.**;
- Metodológia PRIPARE Príloha C: Zoznam princípov, smerníc a kontrol súkromia pre zapojenie požiadaviek do praxe**Error! Reference source not found.**;
- Ochrana údajov a súkromia ENISA na základe projektu**Error! Reference source not found.** obsahuje odkazy na veľký počet PET;

Zapojenie všetkých účastníkov počas technického procesu

Pred začiatkom technického procesu by sa mali všetci účastníci identifikovať („tí, ktorí sú alebo by mohli byť zainteresovaní na alebo ovplyvnení projektom, technológiou, službou“**Error! Reference source not found.**), napr. koncví používateľa, dátové

subjekty, orgány ochrany údajov, poskytovatelia služieb, operátori systému a projektanti.

Všetky skupiny účastníkov by mala zastupovať osoba počas špecifických aktivít technického procesu, ktorá umožňuje viacero pohľadov na systém a potenciálne otázky súkromia, ktoré sa vzťahujú na každú skupinu. Každá skupina účastníkov poskytne svoju vlastnú sústavu požiadaviek, ktoré budú súčasťou procesu porovnávania počas fázy projektu.

Účastníci môžu byť zároveň súčasťou procesu dizajnu a môžu sa ozvať vždy, keď sa budú prejednávať významné rozhodnutia ohľadom realizovateľnosti požiadaviek alebo prístupov, čo umožní diskusiu medzi viacerými účastníkmi a pomôže pravdivo si zvoliť vhodné porovnania.

A v neposlednom rade, ak systém overí viacero účastníkov a vypracuje verejnú správu, odsúhlasením činností súkromia vykonávaných počas technického procesu sa poskytne miera transparentnosti, ktorá pomôže zvýšiť úroveň dôvery v daný systém.

Transparentnosť

Transparentnosť, jeden zo základných princípov PbD, je kľúčom k odstráneniu bariér dôvery, ktoré bránia prijímaniu nových systémov ICT. Technický proces by mal jasne ukazovať, aké sú hlavné technické rozhodnutia spojené so súkromím, osobné údaje sa získavajú, ukladajú alebo spracovávajú v systéme, ochranné prvky sú zavedené pre ochranu takýchto údajov a všetky identifikované riziká (adresované a zvyšné), ktoré boli identifikované počas technického procesu, preukazujúce zhodu s existujúcim právnym rámcom.

Verejná správa, ktorá uvádza všetky tieto informácie (keď je to možné a podľa pravidiel IPR a bezpečnostnej politiky), by sa mala zdieľať s dátovými subjektmi a dozornými orgánmi a orgánmi ochrany údajov.

Požiadavky na transparentnosť by sa mali prejednať s účastníkmi počas fázy analýzy a mali by sa zväžiť v rámci politiky súkromia organizácie.

Zameranie na používateľa

Zameranie na používateľa je preťažený termín, pokiaľ ide o systémy ICT a súkromie. Na jednej strane sú systémy zamerané na používateľa tie systémy, ktoré sú vypracované s individuálnymi používateľmi, pri zohľadnení ich aspektov súkromia a sociekonomických vlastností cielených používateľov počas návrhu systému. Na druhej strane, zameraie na používateľa sa dá uinterpretovať ako oprávnenie používateľa, ktoré umožňuje samostatné určenie a „celkovú“ kontrolu nad ich osobnými údajmi. Obidva prístupy sú významné a mali by sa zväžiť počas technického procesu zameraním sa na vylúčenie požiadaviek spojených so súkromím a počas návrhu systému, najmä v zmysle aspektov používateľského rozhrania (UI).

Podľa štúdie pre pochopenie spotrebiteľov za účelom navrhnutiaproductov a služieb, ktoré vytvárajú dôveru v značky **Error! Reference source not found.**, existuje šesť princípov návrhu zameraných na používateľa, ktoré je potrebné vziať do úvahy:

- Kontext: aké sú mentálne modely používateľov, presvedčenia, očakávania a toky úloh?
- Motivácia: čo zaujíma používateľov?
- Povedomie: vedia používatelia, že existuje?
- Schopnosť odhalenia: ak ju hľadajú, nájdu ju používatelia?
- Pochopenie a uchovanie: chápu používatelia a pamätajú si? Dokážu opakovať procesy?
- Použitelnosť: Dokážu používatelia interagovať?

Rovnaká štúdia stanovila, že dva hlavné faktory, o ktoré sa zákazníci viac starajú, predstavovali:

- Transparentnosť: „Že je jasné, čo sa deje počas používania služby Že nezistia príčinu po udalosti alebo z iného zdroja“
- Voľba: „Že si dokážu zvoliť prvky, ktoré sa dajú ovládať počas služby alebo rozhodnutie o používaní tejto služby“

Zameranie na používateľa je teraz náročnejšie ako kedykoľvek predtým, keďže služby ICT sa používajú na základe zariadení s malým faktorom, s obrazovkami obmedzenej veľkosti a dokonca aj bez nich (napr. Internet of Things).

Súkromie musí pokrývať celý cyklus životnosti technických a osobných údajov

Súkromie nepredstavuje samostatný proces a nedá sa spájať s jedinečnou fázou technického procesu. Aspekty súkromia sa musia zväžiť v každej technickej fáze, aby sa efektívne zaviedli overiteľné opatrenia súkromia (technické alebo organizačné), ktoré riešia požiadavky súkromia, ktoré pramenia z právneho rámca, stanovísk akcionárov, z organizačných vlastných politík a z moderných najlepších postupov.

Najlepším spôsobom ako to dosiahnuť na organizačnej úrovni je spojiť špecifické postupy súkromia s existujúcim riadením projektu a vypracovávaním organizačných procesov. PRIPARE obsahuje vo svojej metodológii **Error! Reference source not found.** (Príloha A) smernice o tom ako sa dajú aktivity súkromia spájať s tradičnými a modernými technickými metodológiami softvéru (napr. waterfall alebo scrum).

Okrem zamerania na súkromie počas celého cyklu životnosti sa musí zväžiť aj cyklus životnosti osobných údajov, osobné údaje sa musia nielen chrániť, keď sa ukladajú, ale princípy súkromia a ochrany údajov (napr. informovaný súhlas) sa musia zväžiť počas získavania, spracovania a dokonca aj počas „likvidácie“ osobných údajov. Požiadavky súkromia môžu a mali by byť špecificky spojené s niektorou fázou cyklu životnosti osobných údajov.

Nasledujúce smernice sú nastavené na rôzne fázy cyklu životnosti.

Popis vysokej úrovne a úvodné hodnotenie (Analýza)

Prvým krokom každého technického procesu je mať jasný pohľad na systém a na to, aké sú obchodné ciele. Počas procesu konzultácie by mali všetci účastníci poskytnúť svoj vlastný pohľad na systém, ktorý by mal byť na základe dohody konsolidovaný a mal by slúžiť ako základ pre diskusie spojené so súkromím. Konštrukcia tohto úvodného pohľadu môže byť podporená vypracovaním vhodného grafického znázornenia (napr. diagramy

obchodného procesu) - Tieto znázornenia by mali byť technologicky nezávislé a prítomné na vysokej úrovni, čo sa vzťahuje na osobné údaje, ktoré sa budú získavať, spracovávať a ukladať a aj na väčšie dátové toky v systéme.

Na základe tohto popisu vysokej úrovne môžu účastníci zadávať svoje otázky ohľadom súkromia, právní odborníci môžu začať identifikovať právny rámec a odborníci na súkromie môžu začať budovať základnú líniu požiadaviek súkromia a identifikovať riziká súkromia. Hľadaním v tejto fáze sa stanoví nespojitosť ďalšej analýzy a činností v oblasti súkromia (napr. systémy s veľmi nízkymi rizikami súkromia nemusia mať rovnaké potreby ako iné, keď sú zapojené citlivé údaje)

Tento úvodný pohľad (s príslušnými grafickými znázorneniami) by sa nemal považovať za obmedzenie procesu návrhu, ale za začiatok významných diskusií medzi účastníkmi.

Tieto smernice sú spojené s odporúčaniami projektu PIAF **Error! Reference source not found.** a metodológiou PRIPARE **Error! Reference source not found.** Proces „Funkčného popisu a vysokej úrovne“.

Príprava plánu súkromia

Keď budete mať jasný pohľad na celý systém, keď identifikujete jeho hlavné ciele a riziká, musíte pripraviť plán súkromia. Takýto plán, ktorý bude riadiť činnosti súkromia počas trvania projektu, sa musí nastaviť podľa plánov na úrovni organizácie a musí stanoviť:

- Presné činnosti súkromia a ich očakávané výstupy;
- Tím súkromia, ktorý bude vykonávať činnosti súkromia s jasnými úlohami a povinnosťami;
- Zoznam a rozsah činností súkromia s prideleným rozpočtom a časovým rámcom

Presný tím, rozsah a činnosti sa určia na základe zistení počas úvodného hodnotenia podľa politiky organizácie, ktorá môže vyplývať z metodológie PRIPARE **Error! Reference source not found.** procesu „Predbežných činností“ a odporúčaní PIAF ohľadom „Analýzy prahu“ **Error! Reference source not found.**

PRIPARE **Error! Reference source not found.** a rámec RFID PIA **Error! Reference source not found.** poskytujú vlastné strom rozhodnutí pre stanovenie rozsahu PIA a dá sa uviesť ako príklad. Tento strom rozhodnutí by mal zohľadniť špecifické body domény a bežné kategórie osobných údajov a riziká (ako je to uvedené v bode **Error! Reference source not found.**).

Požiadavky súkromia

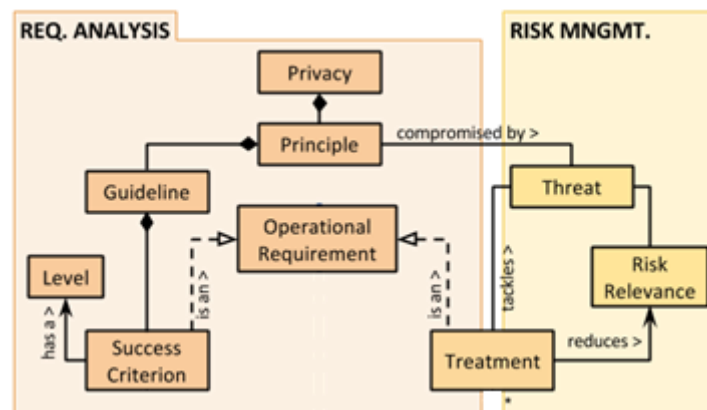
Skutočným cieľom budovania systému je poskytnúť systém, ktorý plní očakávania svojich účastníkov. Proces budovania by mal stanoviť porovnanie pre vyváženie protichodných očakávaní. Hlavným prostriedkom zachytenia týchto očakávaní sú požiadavky (funkčné a nefunkčné). Zachovávanie súkromia komplexnej oblasti s takouto kontextuálnou hodnotou, správna identifikácia požiadaviek, ktoré splnia očakávania a potreby účastníkov, je náročné a „stále nepredstavuje jednotný pohľad na vytváranie požiadaviek súkromia“ **Error! Reference source not found.**

Požiadavky súkromia sa môžu zdefinovať v závislosti od ich podstaty ako funkčné požiadavky (napr. právny rámec si môže vyžadovať, aby boli všetky osobné údaje

prístupné pre dátové subjekty) alebo nefunkčné (napr. vyjadrujúce obmedzenia v zmysle metriky súkromia).

Ako to navrhuje PRIPARE **Error! Reference source not found.**, dajú sa skombinovať dva hlavné prístupy pre identifikáciu prevádzkových požiadaviek súkromia, zamerané na cieľ (pozrite si časť 0) a založené na riziku (pozrite si časť 0), aby sa dosiahli výhody oboch z nich:

- Položky zamerané na cieľ **Error! Reference source not found.**
 - „dodržujú systematický prístup využívajúci katalógy ako prostriedok prenosu princípov vysokej miery súkromia do prevádzkových požiadaviek súkromia“
 - „definujú hrozby v zmysle skutočností, ku ktorým sa dostanete bez akejkoľvek neistoty, bez ohľadu na pravdepodobnosť výskytu“
 - „výber požiadaviek a ich špecifikácia podľa miery požadovanej ochrany podporujú systémy, ktoré ponúkajú nízku, strednú alebo vysokú ochranu osobných údajov“
- Položky založené na riziku
 - Riešia špecifické body vytvoreného systému;
 - Poskytujú hlbšie pochopenie zraniteľných miest a hrozieb systému.



Obrázok 10: Proces navrhovaný PRIPARE **Error! Reference source not found.**

Oba prístupy vychádzajú z výberu princípov súkromia na vysokej úrovni. Tieto princípy by mali predstavovať rozšírenie princípov zadefinovaných rámcom nariadení, rozšíreným o každý princíp, ktorý vynútil niektorý z účastníkov. Takisto sa odporúča spájať všetky požiadavky súkromia s ich zdrojom: účastník, princíp na vysokej úrovni, smernica alebo hrozba, zaistenie vysledovateľnosti a zodpovednosti celej analýzy súkromia a procesu projektu.

Projekt súkromia

Po definícii zvolenej pre PRIPARE v časti D1.1 **Error! Reference source not found.** je projekt systému „proces zadefinovania hardvérovej a softvérovej architektúry, komponentov, modulov, rozhraní a údajov pre systém pre dodržanie uvedených požiadaviek“.

Navrhnutie systému nie je jednoduchá činnosť, dá sa považovať za proces pozostávajúci z viacerých disciplín, kde je systém navrhnutý z viacerých pohľadov. Pokiaľ ide o súkromie, existujú tri hlavné pohľady, ktoré je potrebné zvážiť:

- **Architektonický:** architektúry systému sú kľúčom k úrovniám súkromia, ktoré sa dajú v ich rámci dosiahnuť. Nesprávna voľba na architektonickej úrovni môže obmedzovať vzorce súkromia, ktoré sa dajú zvoliť alebo ktoré sú kompatibilné s PET. Navrhuje sa teda dodržiavať reťazový prístup, ktorý hodnotí viacero stratégií alebo vzorcov a vyberať si ich podľa ich výkonnosti vo zvolených scenároch, ako je to uvedené v PEARs **Error! Reference source not found.**
- **Podrobný projekt:** keďže prístup zameraný na cieľ (časť 0) vynucuje katalóg smerníc súkromia a požiadaviek, projektový prístup by mohol využívať katalóg opatrení alebo techník spojených so smernicami súkromia a požiadavkami, ktoré by popisovali technologické špecifické prístupy pre riešenie bežných požiadaviek súkromia. Táto činnosť je popísaná v procese metodológie PRIPARE „Podrobný projekt podporujúci súkromie“ **Error! Reference source not found.** a dá sa považovať za viac nespojitý architektonický projekt navrhovaný v architektonickom pohľade.
- **Používateľské rozhranie:** ako je to uvedené v smernici zameranej na používateľa, používateľské rozhranie predstavuje kritické zvýšenie dôvery používateľov v systém ICT. ISO 9241-210:2010 **Error! Reference source not found.** je norma, ktorá už rieši projekt zameraný na ľudí a ktorá sa dá použiť pre požiadavky alebo aspekty špecifické pre súkromie.

Keď máme vypracovaný základný projekt, mal by sa overiť na základe požiadaviek, ktoré sa vyvolali počas predchádzajúcich činností. Proces projektovania do značnej miery využíva inventáre alebo katalógy vzorcov súkromia, PET, technické alebo organizačné opatrenia, ktoré sa navrhli v smernici „Vytvorenia štruktúry súkromia na organizačnej úrovni“.

Implementácia a overenie súkromia

Súkromie sa rieši na úrovni implementácie systému implementáciou špecifických mechanizmov súkromia a PET, ktoré dsa zvolili a zaviedli do architektúry alebo podrobného projektu počas fázy projektu. Na tejto úrovni je maximálne dôležité dodržiavať smernice o technologickej implementácii súkromia špecifické pre daný jazyk, ako sú:

- Najlepšie postupy Android pre bezpečnosť a súkromie **Error! Reference source not found.**
- Bezpečnostná príručka iOS **Error! Reference source not found.**
- Bezpečnostná príručka Red Hat Enterprise Linux 6 **Error! Reference source not found.**
- Smernice bezpečného vývoja smartphonov ENISA pre vývojárov aplikácií **Error! Reference source not found.**
- OWASP Secure Coding Practices Quick Reference Guide **Error! Reference source not found.**

Na úrovni overenia sa nachádza viacero prístupov:

- Statická analýza: implementácia systému (napr. zdrojový kód alebo dokumentácia) sa dá manuálne alebo automaticky skontrolovať podľa organizačnej alebo projektovej politiky, aby sa stanovilo, či implementácia rieši dohodnuté požiadavky a aby sa zistili potenciálne problémy bezpečnosti alebo súkromia (napr. overenia statického kódu pri hľadaní zraniteľnosti bezpečnosti **Error! Reference source not found.**)
- Dynamická analýza: pred alebo počas využívania systému sa prevádzkový systém testuje, pričom sa hľadajú zraniteľné miesta v dobre zvolených scenároch testu. Prístupy testovania prieniku **Error! Reference source not found.**, automatické generovanie testu **Error! Reference source not found.** a overovanie súkromia času chodu **Error! Reference source not found.** sú výkonné prostriedky pre túto činnosť.

Navrhovaný prístup pre riešenie implementácie súkromia a overenie je stanovenie procesu „súvislého overovania“ (analogicky so súvislou integráciou), kde sa napredovanie implementácie neustále overuje a odhalia sa všetky problémy súkromia a bezpečnosti v skorej fáze procesu implementácie (čím sa minimalizujú náklady).

Kontroly súkromia systému pred jeho prevádzkou

Rovnako ako pred presunom systému do výrobného prostredia, najlepšie technické postupy umožňujú vypracovanie účinného plánu obnovy, najlepšie technické postupy súkromia odporúčajú vypracovanie:

- Plánu reakcie na incidenty s jasnými úlohami, zodpovednosťami a postupmi pre reakciu na incident bezpečnosti alebo súkromia v dôsledku porušenia súkromia. Takýto plán by mal obsahovať jasné smernice o tom, kedy kontaktovať orgán pre ochranu údajov. Článok 29 uvádza niektoré príklady **Error! Reference source not found.**, ktoré ukazujú, za akých podmienok sa musia DPA a dátové subjekty informovať. Rada štátnej pokladnice kanadského sekretariátu zverejnila svoju „spravu nástrojov riadenia v prípade porušenia súkromia“ **Error! Reference source not found.**, ktorá sa dá použiť ako referencia.
- Plánu vyradenia systému z prevádzky, kde sa zohľadnia údaje, ktoré sa budú získavať a uložia sa v systéme, ako aj ich príslušné riziká, postupy, ktoré sa budú dodržiavať, keď sa systém vyradí z prevádzky. Podľa právnych rámcov to môže zahŕňať informovanie zákazníkov, čo im umožní získať ich osobné údaje a zlikvidovať a/alebo anonymizovať údaje.
- Konečnej revízie všetkých dodržiavaných činností súkromia, pri kontrole úvodného plánu súkromia, zaistení toho, že sa budú všetky výstupy zhodovať s ich pôvodnou špecifikáciou.
- Verejnej správy, ktorá informuje o aspektoch súkromia systému podľa popisu v smernici „Transparentnosť“.

Prevádzka a vyradenie systému z prevádzky spojeného so súkromím

PbD sa neskončí, keď sa systém dostane do výroby. Počas prevádzky systému by sa mali vyskytovať opakujúce sa činnosti s cieľom zaistiť správnu prevádzku plánovaných a implementovaných opatrení súkromia. Ako sa to navrhuje v metodológii PRIPARE „Overenia bezpečnosti a súkromia“ **Error! Reference source not found.**, niektoré

činnosti, ktoré sa dajú použiť na zaistenie prevádzky spojenej so súkromím systému sú nasledovné:

- Opätovne preskúmajte modely hrozieb, správy o analýze a výsledky testov
- Skontrolujte plány vyradenia z prevádzky a reakcie
- Zaistite, že kontroly súkromia sú zavedené a fungujú podľa očakávaní
- Skontrolujte a zaistite, aby bola dokumentácia presná

Napokon a po vyradení systému z prevádzky sa musí dodržať plán vyradenia z prevádzky, ktorý zaistí správne uloženie alebo likvidáciu všetkých príslušných osobných údajov.

9 Preukázanie výhod PbD

PbD je celkom mladá oblasť a technický prístup k nej je ešte mladší. Hľadanie úspešných referencií na úspešné skutočné použitia takýchto postupov je výzvou. Táto kapitola teda zostavuje referencie o postupoch PbD, ktoré, aj keď sa ešte neuplatňujú v prevádzkovom prostredí, poskytujú dôkaz o tom aký významný vplyv má technický proces PbD na spôsob, akým dokážu navrhované systémy chrániť súkromie dátového subjektu. V tejto kapitole sa používajú domény smart grid a Internet of Things, ktoré ukazujú tieto výhody. Táto kapitola uvádza prístupy PRIPARE a LINDDUN na preukázanie výhod.

9.1 Smart Grid

V priebehu nasledujúcich rokov smart metering a smart grids vynúti existujúce postupy ako napríklad:

- Vzorce dopytu sa zmenia v dôsledku zvyšujúceho sa prijímania elektrifikácie alebo technológií ako je preprava, zahrievanie, ukladanie batérie.
- Prijímanie zelených zdrojov energie stabilizuje generovanie energie a zaisťuje jej plynulejšiu geografickú distribúciu

V dôsledku tejto predpovede poskytovatelia energie a sietí vypracovávajú smart grids, ktoré dokážu vyvážiť dopyt energie takmer v reálnom čase. Meranie dopytu energie v reálnom čase však prináša mnoho problémov so súkromím. Vytváranie súkromia je značne zamerané na smart grid. Medzi niektoré relevantné práce vytvárania súkromia, ktoré preukazujú výhody vytvárania PbD, patria:

- Hodnotenie vplyvu na súkromie, ktoré sa vykonalo v mene asociácie energetických sietí **Error! Reference source not found..** Tento PIA úspešne identifikuje hlavné riziká súkromia a problémy akcionárov a vypracováva sústavu odporúčaní na ich riešenie.
- OASIS PMRM **Error! Reference source not found.:** obsahuje vo svojom popise príklad prípadu používania („Všestranný inteligentný systém nabíjania elektrického vozidla“), ktorý sa používa na preukázanie výhod používania PMRM v systéme ICT citlivom na súkromie. PRIPARE, počas svojho posledného roku prevádzky, použil časť svojej holistickej metodológie na rovnaký prípad používania s cieľom preukázať použiteľnosť a výhody tejto metodológie. Táto práca sa ešte musí zverejniť na webovej stránke PRIPARE **Error! Reference source not found..**
- POPCORNE **Error! Reference source not found.:** použitím prístupu PIA na vozidlo ISO pri komunikačnom rozhraní mriežky **Error! Reference source not found.** sa vypracoval protokol nabíjania chrániaci súkromie, ktorý dodržiava všetky funkcie ISO15118 a preukazuje výhody uplatňovania PIA.

9.2 Internet of Things

Článok 29 vydal v roku 2014 stanovisko k nedávnomu rozvoju v oblasti Internet of Things **Error! Reference source not found.**, kde označuje Internet of Things (IoT) ako „infraštruktúru, v ktorej sa nachádzajú miliardy snímačov zakódovaných v bežných, každodenných zariadeniach – „things“ ako takých alebo things spojených s ostatnými

objektmi alebo osobami – je navrhnutý na zaznamenávanie, spracovávanie, ukladanie a prenos údajov a keďže je spojený s jedinečnými identifikátormi, interaguje s ostatnými zariadeniami alebo systémami využívajúcimi schopnosti siete”.

Tieto „things“ môžu predstavovať mnohé výzvy bezpečnosti a súkromia. Mnohé z nich nemajú alebo majú obmedzené fyzické rozhrania používateľa, majú obmedzený výkon spracovávania (bránia používaniu komplexných kryptografických techník) a môžu sa veľmi ťažko aktualizovať. Článok 29 dodržiava prístup hodnotenia rizika súkromia, aby sa zistili potenciálne problémy, opatrenia a odporúčania, spojené s európskym právnym rámcom, ktorý by mali zväžiť účastníci odvetvia IoT.

IoT-AError! Reference source not found. je projekt spolu financovaný EÚ a je súčasťou programu FP7, ktorý vypracoval „architektonický referenčný model pre vzájomnú prevádzkyschopnosť systémov Internet-of-Things, načrtol princípy a smernice pre technický projekt svojich protokolov, rozhraní a algoritmov“. Ak sa majú riešiť socioekonomické aspekty súkromia architektúry a technológie, tento projekt vykonal PIA na základe rámca BSI PIA **Error! Reference source not found.**, pričom úspešne identifikoval kontroly, ktoré sa musia zaviesť pre odstránenie, zmiernenie alebo prenos detegovaných rizík.

9.3 LINDDUN

LINDDUN obsahuje, v rámci svojho pôvodného popisu**Error! Reference source not found.**, prílohu, ktorá preukazuje ako úspešne sa uplatňuje vo fiktívnom scenári sociálnej skupiny pre identifikáciu opatrení, ktoré môžu byť súčasťou projektu, aby sa zabránilo materializácii hrozieb súkromia.

9.4 PRIPARE

V kontexte projektu PRIPARE sme kontaktovali ďalšie tri projekty na úrovni EÚ a navrhli sme použiť PRIPARE v istej fáze projektu s dvojitým cieľom a) preukázať použiteľnosť a užitočnosť prístupu PRIPARE a b) zhodnotiť a zvýšiť mieru súkromia dosahovanú v technologických výstupoch projektov. Zatiaľ čo výsledky tejto iniciatívy ešte nie sú zverejnené, na základe tejto spolupráce sa vypracoval rámec vytvárania súkromia špecifický pre IoT**Error! Reference source not found.**, podľa princípov PRIPARE, pričom sa preukázalo, že sa prijali výhody prístupu PRIPARE.

10 Referencie

- [1] European Data Protection Supervisor (EDPS). EDPS - Glossary - Accountability. [Online].
<https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability>
- [2] International Organization for Standardization (ISO), "ISO/IEC 29100:2011 - Information technology -- Security techniques -- Privacy framework," Genève, Standard 2011.
- [3] Article 29 Data Protection Working Party, "Opinion 05/2014 Anonymisation Techniques," April 2014.
- [4] European Parliament and the Council, "Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281," 23.11.1995.
- [5] European Parliament and the Council, "Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community,".
- [6] European Data Protection Supervisor (EDPS). EDPS - Glossary - Consent.
- [7] Article 29 Data Protection Working Party, "Working Document 02/2013 providing guidance on obtaining consent for cookies," October 2013.
- [8] European Data Protection Supervisor (EDPS). EDPS - Glossary - Data minimisation. [Online].
https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74#data_minimization
- [9] PRIPARE, "Deliverable D1.1 Privacy and Security, Concepts and Principles Report," 2014.
- [10] European Data Protection Supervisor (EDPS). EDPS - Glossary - Data subject. [Online].
https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74#data_subject
- [11] European Data Protection Supervisor (EDPS). EDPS - Glossary - Privacy. [Online].
<https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/84#privacy>
- [12] Information and Privacy Commissioner of Ontario (IPC). Introduction to Privacy by Design. [Online]. <https://www.ipc.on.ca/english/privacy/introduction-to-pbd/>
- [13] Commission nationale de l'informatique et des libertés (CNIL), "Methodology For Privacy Risk Management," 2012.
- [14] Daniel Le Métayer, "IT Security Analysis Best Practices and Formal Approaches," in *Foundations of Security Analysis and Design*. Berlin, Germany: Springer, 2007,

pp. 75-91.

- [15] International Organization for Standardization (ISO), "ISO/IEC 15408-1:2009 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model," Geneve, 2009.
- [16] Rajeev Motwani and Ying Xu, "Efficient Algorithms for Masking and Finding," 2007.
- [17] Ann Cavoukian, "Foundational Principles of Privacy by Design," Information & Privacy Commissioner of Ontario, Canada,. [Online]. <http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/>
- [18] 32nd International Conference of Data Protection and Privacy Commissioners, "Privacy by Design Resolution," Jerusalem, Israel, 2010.
- [19] C Gonzalez Troncoso, C Diaz S Gürses, "Engineering Privacy by Design," in *Computers, Privacy & Data Protection*, 2010.
- [20] David Wright, and Michael Friedewald Rachel L. Finn, "Seven Types of Privacy," in *European Data Protection: Coming of Age.*, 2013.
- [21] Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review*, vol. 25, pp. 123-135, April 2009.
- [22] Information Commissioner's Office (ICO), "Privacy Impact Assessment Handbook," UK, Version 2.0, 2009.
- [23] RFID Industry, "Privacy and Data Protection Impact Assessment Framework for RFID Applications," January 2011. [Online]. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf
- [24] Bundesamt für Sicherheit in der Informationstechnik, "Privacy Impact Assessment Guideline," 2011.
- [25] European Commision, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals.(General Data Protection Regulation),".
- [26] Commission nationale de l'informatique et des libertés (CNIL), "Privacy Impact Assessment (PIA) - Methodology (how to carry out a PIA),".
- [27] PIAF (A Privacy Impact Assessmen Framework), "Deliverable D3 - Recommendation for a privay impact assessment framework for the European Union," 2012.
- [28] Organization for the Advancement of Structured Information Standards (OASIS), "Privacy Management Reference Model and Methodology (PMRM)," v1.0, July

2013. [Online]. <http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.pdf>
- [29] Organization for the Advancement of Structured Information Standards (OASIS), "Privacy by Design Documentation for Software Engineers (PbD-SE) Technical Committee," [Online]. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se
- [30] Organization for the Advancement of Structured Information Standards (OASIS), "Privacy by Design Documentation for Software Engineers," Draft Version 1.0, [Online]. <http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.html>
- [31] Institute for Computer Sciences and Technology National Bureau of Standards, "Guidelines for Automatic Data Processing Physical Security and Risk Management," Federal Inf. Process. Stds. (NIST FIPS) - 31, June 1974.
- [32] Kim Wuyts, "Privacy Threats in Software Architectures," 2015.
- [33] Microsoft. The STRIDE Threat Model. [Online]. <https://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx>
- [34] LINDDUN. Privacy threat trees catalog. [Online]. <https://distrinet.cs.kuleuven.be/software/linddun/catalog.php>
- [35] LINDDUN. Mitigation Strategies & Solutions. [Online]. <https://distrinet.cs.kuleuven.be/software/linddun/solutions.php>
- [36] National Institute of Standards and Technology (NIST), "Privacy Risk Management for Federal Information Systems," NISTIR 8062 (Draft), 2015. [Online]. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf
- [37] PRIPARE. PRIPARE. [Online]. <http://pripareproject.eu/>
- [38] N. Notario et al., "PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology," in *Security and Privacy Workshops (SPW), 2015 IEEE*, May 2015, pp. 151-158.
- [39] W3C. Web Content Accessibility Guidelines. [Online]. <http://www.w3.org/WAI/intro/wcag>
- [40] W3C. How WAI Develops Accessibility Guidelines through the W3C Process. [Online]. <http://www.w3.org/WAI/intro/w3c-process.php>
- [41] Microsoft. Microsoft Security Development Lifecycle. [Online]. <https://www.microsoft.com/en-us/sdl/>
- [42] Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna, "PiOS: Detecting Privacy Leaks in iOS Applications," in *Network and Distributed System Security Symposium*, 2011.

- [43] Peter Gilbert, Byung-gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth William Enck, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," in *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, , Vancouver, 2010.
- [44] Open Web Application Security Project (OWASP). [Online]. <https://www.owasp.org>
- [45] Open Web Application Security Project (OWASP). Software Assurance Maturity Model. [Online]. [https://www.owasp.org/index.php/Category:Software Assurance Maturity Model](https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model)
- [46] Open Web Application Security Project (OWASP). Application Security Verification Standard (ASVS). [Online]. [https://www.owasp.org/index.php/Category:OWASP Application Security Verification Standard Project](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)
- [47] Open Web Application Security Project (OWASP), "OWASP Secure Coding Practices Quick Reference Guide," Version 2.0, November 2010. [Online]. [https://www.owasp.org/images/0/08/OWASP SCP Quick Reference Guide v2.pdf](https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf)
- [48] Open Web Application Security Project (OWASP). OWASP Security Principles Project. [Online]. [https://www.owasp.org/index.php/OWASP Security Principles Project](https://www.owasp.org/index.php/OWASP_Security_Principles_Project)
- [49] Open Web Application Security Project (OWASP). OWASP Risk Rating Methodology. [Online]. [https://www.owasp.org/index.php/OWASP Risk Rating Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)
- [50] Open Web Application Security Project (OWASP). OWASP Testing Project. [Online]. [https://www.owasp.org/index.php/OWASP Testing Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
- [51] International Organization for Standardization (ISO), "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements," 2013.
- [52] International Organization for Standardization (ISO), "ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls," 2013.
- [53] ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. [Online]. <http://www.isaca.org/cobit/pages/default.aspx>
- [54] Payment Card Industry - Data Security Standards Council. PCI SSC Data Security Standards Overview. [Online]. https://www.pcisecuritystandards.org/security_standards/index.php
- [55] Google. Best Practices for Security & Privacy. [Online].

<http://developer.android.com/training/best-security.html>

- [56] Apple, "iOS Security—White Paper - iOS 9.0 or later," September 2015. [Online]. https://www.apple.com/business/docs/iOS_Security_Guide.pdf
- [57] Red Hat Enterprise. Red Hat Enterprise Linux 6 Security Guide - A Guide to Securing Red Hat Enterprise Linux. [Online]. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/
- [58] European Union Agency for Network and Information Security (ENISA), "Smartphone Secure Development Guidelines," 2011. [Online]. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines/at_download/fullReport
- [59] Cloud Security Alliance (CSA). Cloud Controls Matrix Working Group. [Online]. <https://cloudsecurityalliance.org/group/cloud-controls-matrix/>
- [60] International Organization for Standardization (ISO), "ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework,". [Online]. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123
- [61] International Organization for Standardization (ISO), "• ISO/IEC 29101:2013 Information technology -- Security techniques -- Privacy Architecture framework," 213.
- [62] International Organization for Standardization (ISO), "ISO/IEC CD 29134 - Privacy impact assessment -- Methodology," (Under development),.
- [63] International Organization for Standardization (ISO), "ISO/IEC CD 29151 -- Code of practice for PII protection," (Under development),.
- [64] MITRE PRivacy Community of Practice (CoP), "Privacy Engineering Framework," 2014.
- [65] Article 29 Working Party. [Online]. http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
- [66] Article 29 Data Protection Working Party, "Opinion 03/2014 on Personal Data Breach Notification," March 2014.
- [67] Article 29 Data Protection Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things," 2014.
- [68] Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks,". [Online]. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion->

[recommendation/files/2014/wp218_en.pdf](#)

- [69] Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner George Danezis, "Privacy and Data Protection by Design – from policy to engineering," European Union Agency for Network and Information Security (ENISA), 2014.
- [70] European Network and Information Security Agency (ENISA), "The new users' guide: How to raise information security awareness," November 2010.
- [71] European Parliament, "Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ,".
- [72] Mozilla. Privacy Icons. [Online]. https://wiki.mozilla.org/Privacy_Icons
- [73] Disconnect.me. Privacy Icons. [Online]. <https://disconnect.me/icons>
- [74] Google. Personal info & privacy. [Online]. <https://myaccount.google.com/privacy>
- [75] W3C. Privacy Dashboard. [Online]. <http://code.w3.org/privacy-dashboard/>
- [76] Privowny. [Online]. <https://privowny.com/>
- [77] PrimeLife, "End User Transparency Tools: UI Prototypes," 2010. [Online]. http://primelife.ercim.eu/images/stories/deliverables/d4.2.2-transparency_tools_ui_prototypes-public.pdf
- [78] Mozilla. Lightbeam. [Online]. <https://www.mozilla.org/es-ES/lightbeam/>
- [79] Terms of Service; Didn't Read. [Online]. <https://tosdr.org/>
- [80] Electronic Frontier Foundation. Panopticllick. [Online]. <https://panopticllick.eff.org/>
- [81] F-Secure. App Permissions. [Online]. https://www.f-secure.com/en/web/home_global/app-permissions
- [82] W3C. Platform for Privacy Preferences (P3P) Project. [Online]. <http://www.w3.org/P3P/>
- [83] AdBlockPlus. [Online]. <https://adblockplus.org/>
- [84] Ghostery. [Online]. <https://www.ghostery.com/en/>
- [85] W3C, "Tracking Preference Expression (DNT)," W3C Candidate Recommendation 20 August 2015. [Online]. <http://www.w3.org/TR/2015/CR-tracking-dnt-20150820/>

- [86] IBM. Identity Mixer. [Online]. <http://www.zurich.ibm.com/idemix/>
- [87] Microsoft. U-Prove. [Online]. <http://research.microsoft.com/en-us/projects/u-prove/>
- [88] Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold William Aiello, "Just fast keying: Key agreement in a hostile internet," *ACM Transactions on Information and System Security (TISSEC)*, vol. 7, no. 2, pp. 242-273, May 2004.
- [89] STORK. [Online]. <https://www.eid-stork.eu/>
- [90] Sibboleth. [Online]. <https://shibboleth.net/>
- [91] Attribute-based Credentials for Trust (ABC4Trust). [Online]. <https://abc4trust.eu/>
- [92] The International PGP Home Page. [Online]. <http://www.pgpi.org/>
- [93] Internet Engineering Task Force (IETF), "ZRTP: Media Path Key Agreement for Unicast Secure RTP,". [Online]. <http://tools.ietf.org/html/rfc6189>
- [94] Whisper Systems, "Open Whysper Systems,". [Online]. <https://whispersystems.org/>
- [95] David L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84-90, February 1981.
- [96] Baiyu Li, Mohammad Derakhshani, and Ian Goldberg Hooman Mohajeri Moghaddam, "SkypeMorph: protocol obfuscation for Tor bridges," *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 97-108, 2012.
- [97] Google. Full Disk Encryption. [Online]. <https://source.android.com/devices/tech/security/encryption/>
- [98] Apple. OS X Yosemite: Encrypt the contents of your Mac with FileVault. [Online]. https://support.apple.com/kb/PH18637?locale=en_US&viewlocale=en_US
- [99] TrueCrypt. [Online]. <http://truecrypt.sourceforge.net/>
- [100] Microsoft. BitLocker Drive Encryption Overview. [Online]. <http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview>
- [101] The Guardian Project. LUKS: Disk Encryption. [Online]. <https://guardianproject.info/code/luks/>
- [102] Boxcryptor. Encrypt your files in your Dropbox. [Online].

<https://www.bboxcryptor.com/en/dropbox>

- [103] J. Domingo-Ferrer and J.M Mateo-Sanz, "Practical data-oriented microaggregation for statistical disclosure control," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 14, no. 1, pp. 189-201, 2002.
- [104] José Gouweleeuw, Peter Kooiman, Leon Willenborg, and Peter-Paul De Wolf, "THE POST RANDOMISATION METHOD FOR PROTECTING MICRODATA," *Qüestió*, vol. 22, no. 1, pp. 145-156, 1998.
- [105] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, pp. 557-570, 2002.
- [106] Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam shwin Machanavajjhala, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discov. Data*, vol. 1, no. 1, p. Article 3, 2007.
- [107] Ninghui Li, Tiancheng Li, and S Venkatasubramanian, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity," in *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on*, 2007, pp. 106-115.
- [108] Helen Nissenbaum, Vincent Toubiana Daniel C. Howe. TrackMeNot. [Online]. <https://cs.nyu.edu/trackmenot/>
- [109] JonDonym. [Online]. <https://anonymous-proxy-servers.net/en/overview.html>
- [110] DuckDuckGo. [Online]. <https://duckduckgo.com/>
- [111] Len Adleman and Michael L. Dertouzos Ronald L. Rivest, "On data banks and privacy homomorphisms," Massachusetts,. [Online]. <http://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf>
- [112] Andrew C. Yao, "Protocols for Secure Computations," California,. [Online]. <http://research.cs.wisc.edu/areas/sec/yao1982-ocr.pdf>
- [113] Andrea Huszti, "A homomorphic encryption-based secure electronic voting scheme," *Publicationes Mathematicae*, vol. 79, no. 3-4, pp. 479-496, 2011.
- [114] Benessa Defend and Klaus Kursawe, "Implementation of privacy-friendly aggregation for the smart grid," in *Proceedings of the first ACM workshop on Smart energy grid security*, New York, 2013, pp. 65-74.
- [115] Sharemind. [Online]. <https://sharemind.cyber.ee/>
- [116] Antonio Kung, "Privacy Enhancing ARchitectures," in *Privacy Technologies and Policy – Second Annual Privacy Forum, APF 2014*, Athens, 2014, pp. 19-29.
- [117] Carnegie Mellon University - Software Engineering Institute. Cost Benefit Analysis Method (CBAM). [Online].

- <http://www.sei.cmu.edu/architecture/tools/evaluate/cbam.cfm>
- [118] Carnegie Mellon University - Software Engineering Institute. Architecture Tradeoff Analysis Method (ATAM). [Online]. <http://www.sei.cmu.edu/architecture/tools/evaluate/atam.cfm>
- [119] Regine Meunier, Hans Rohnert, Peter Sommerlad, and Michael Stal. rank Buschmann, *Pattern-Oriented Software Architecture: A System of Patterns*. New York: John Wiley & Sons, Inc., 1996.
- [120] PRIPARE. privacypatterns.eu - collecting patterns for better privacy. [Online]. <https://privacypatterns.eu/>
- [121] Jaap-Henk Hoepman, "Privacy Design Strategies," 2012. [Online]. <http://arxiv.org/abs/1210.6621>
- [122] PRIPARE, "Deliverable D1.2 Privacy and Security-by-design Methodology," 2015.
- [123] David Wright & Kush Wadhwa, "A step-by-step guide to privacy impact assessment," Privacy Impact Assessment Framework, 2012.
- [124] Create with context, "The Mobile Initiative," 2012.
- [125] PRIPARE, "Deliverable D2.4 - Guidelines for Best Practice Templates," 2015.
- [126] K. Beckers, "Comparing Privacy Requirements Engineering Approaches," in *2012 Seventh Int. Conf. Availability, Reliability and Security*, Aug 2012, p. 574.581.
- [127] Antonio Kung, "PEARs: Privacy Enhancing Architecture," *Privacy Technologies and Policy in Lecture Notes in Computer Science*, vol. 8450, pp. 18-29, 2014.
- [128] International Organization for Standardization (ISO), "ISO 9241-210:2010 - Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems," 2010.
- [129] Bishop Fox. Google Hacking Diggity Project. [Online]. <http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/>
- [130] Open Web Application Security Project (OWASP). Web Application Penetration Testing. [Online]. https://www.owasp.org/index.php/Web_Application_Penetration_Testing
- [131] TrustedLabs. Trusted Labs Computer-Aided Testing (TLCAT). [Online]. <http://trusted-labs.com/security-consulting/tools-training/tl-cat/>
- [132] AppAnalysis. Realtime Privacy Monitoring on Smartphones. [Online]. <http://appanalysis.org/>
- [133] Treasury Board of Canada Secretariat, "Privacy Breach Management Toolkit," [Online]. <https://www.tbs-sct.gc.ca/atip-aiprp/tools/pbmt-togap/pbmt-togapb-b>

[eng.asp](#)

- [134] Engage Consulting Limited, "Privacy Impact Assessment: Use of Smart Metering data by Network Operators," Energy Networks Association, 2011.
- [135] Jonathan Petit, Robert Schmidt, and Frank Kargl Christina Höfer, "OPCORN: privacy-preserving charging for emobility," in *proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles (CyCAR '13)*, pp. 37-48.
- [136] International Organization for Standardization (ISO), "ISO/IEC 15118 - Road vehicles Vehicle-to-Grid - Communication Interface,".
- [137] Internet of Things - Architecture. [Online]. <http://www.iot-a.eu/public>
- [138] Ku Leuven, "LINDDUN: a privacy threat analysis,". [Online]. <https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf>
- [139] Frank Kargl, Santiago Suppan, Jorge Cuellar, Henrich C. Pöhls, Adam Kapovits, Nicolas Notario, Yod Samuel Martin Antonio Kung, "A Privacy Engineering Framework for the Internet of Things," (YET TO BE PUBLISHED),.
- [140] José Gouweleeuw, Peter Kooiman, Leon Willenborg, and Peter-Paul De Wolf, "THE POST RANDOMISATION METHOD FOR PROTECTING MICRODAT," *Qüestiió*, vol. 22, no. 1, pp. 145-156, 1998.
- [141] PrivacyPatterns.org. [Online]. <http://privacypatterns.org/>