Overview of Privacy Guidance for Consumer and Public Interest Representatives
Key Principles

The following document sets out the consumer and public interest privacy principles that are the basis for the detailed good practice requirements provided in the three guidance documents outlined in section 2 of this overview.

1. **Security is fundamental to privacy**.
   Good security prevents unauthorised people from accessing personal information. This principle impinges on
   a. The security of processing platforms used by consumers such as smartphones and tablets as well as home networks
   b. Maintaining consumer processing platforms security in the light of continuous cyber attacks.
   c. The role of the consumer in maintaining their own security and contributing to public network (Internet for example) and private organisation system security

2. **Within the domestic environment consumers should have complete control over their privacy**
   Within your domestic environment the processing undertaken by individuals to help them socialise, run and manage their lives should be secure and under their control wherever the processing is undertaken within the global ICT architecture. For example: fitness apps, home environmental control, travel planning etc.
   This principle impinges on
      a. Home networks and connected devices
      b. Cloud computing services for consumers and use of Cloud services by apps.
      c. Intelligent cars
      d. Parental monitoring and control
      e. Control over socially shared data
      f. Control over intrusive content including SPAM, Porn, online bullying, nuisance calls and more

Ochrana soukromí - Pokyny pro spotřebitele a veřejné zástupce zájmových skupin
Klíčové principy

Následující dokument stanoví zásady spotřebitelů a veřejného zájmu o ochraně osobních údajů. Jsou základem pro detailní požadavky na správnou praxi, zpravované podle řady podrobněji rozvedených dokumentů.

1. **Bezpečnost je zásadní pro ochranu soukromí**

Dobré zabezpečení je obranou před přístupem k osobním údajům neoprávněným osobám. Tento princip se týká
   a. Bezpečnosti procesních platforem sloužících spotřebitelům, jako jsou smartphony a tablety, stejně jako domácí sítě;
   b. Udržování bezpečnosti spotřebitelských procesních platforem s ohledem na kontinuální kybernetické útoky.
   c. Role spotřebitele při udržování jeho vlastní bezpečnosti a při přispívání na veřejné sítě (Internet například) atd.

2. **V rámci svého domácího prostředí musí mít spotřebitel úplnou kontrolu nad ochranou svého soukromí**

V našem domácím prostředí musí být procesní platformy používané jedincem k socializaci, řízení a spravování jeho života bezpečné a naší kontrolou, všude tam, kde je zpracování prováděné v rámci globální architektury informačních a komunikačních technologií. Pro příklad: fitness aplikace, domácí řízení životního prostředí, plánování cest atd.
Tento princip se týká
   a. Domácích sítí a připojených zařízení
   b. Služeb Cloud computing pro spotřebitele a využití služeb Cloud Apps.
   c. Inteligentních automobilů
   d. Rodičovské kontroly a dohledu
   e. Kontroly nad sociálně sdílenými daty
   f. Kontroly nad dotěrným obsahem (včetně spamy, porno, on-line šikana, obtěžující volání a další)

3. When data is collected from consumers then control should be personalised allowing personal privacy preferences to be expressed and changed at any time.

Where consumers consent to data collection as an on going process from domestic activities then real time control over their own privacy preferences is needed. This principle impinges on the data collection for

a. Home health
b. Home environmental control
c. Smart meters and smart grid
d. Traffic and navigation systems
e. Smart Cities
f. The Internet of Things and much more

4. Transparency of data sharing

Transparency of data use shall be ensured when personal data is passed to others. Where individuals have consented to data collection from domestic activities, whether they have explicitly recognised that their data will be passed to and used by others or within a paid for service where data sharing is a necessary part of that service delivery, then there should be transparency enabling the individual to determine who the data has been passed to and for what reason.

5. Personal data analysis processes should be designed to protect individuals privacy

Where personal data is processed in a manner that it is analysed to inform or influence decisions then precautions are needed to protect privacy. This principle impinges on

a. Governance
b. Identifiability
c. Creation of large data sets that collectively represent much more sensitive personal data than individual data items do by themselves
d. Accuracy of analysis, especially false positives and false negatives which impact individuals
e. Use of personal data analysis for personal risk management within health, finance and many other types of service

3. Jsou-li od spotřebitelů získávané údaje, pak jejich kontrola musí být osobní a umožňovat volbu a změny volby ochrany osobních údajů kdykoliv.

Tam, kde spotřebitelé souhlasí se sběrem údajů, jak ve vztahu probíhající procesům z domácích činností, tak v reálném čase, je nezbytná možnost volby vlastním nastavením ochrany osobních údajů. Tento princip se týká sběru dat pro

a. Domácí ochrana zdraví
b. Domácí řízení ochrany životního prostředí
c. Inteligentní měřiče energií
d. Dopravní a navigační systémy
e. Inteligentní města
f. „Internet of Things“

a mnohem víc

4. Transparentnost sdílení dat

Musí být zajištěna transparentnost používání dat, kdy jsou osobní údaje předávány jiným.
I v případě, že jednotlivec souhlasil se sběrem dat z domácích činností, a i výslovně uvedl, že jeho údaje budou předány a použity jinými nebo během provádění služby, kde sdílení dat je nezbytnou součástí tohoto poskytování služeb, pak musí být zajištěna transparentnost umožňující jedinci určit, komu data byla předána a z jakého důvodu.

5. Analýzy procesů osobní údajů musí být navrženy tak, aby bylo chráněno soukromí jednotlivce

Tam, kde jsou osobní údaje zpracovávány formou analýzy s cílem informovat či ovlivňovat rozhodování, pak jsou zapotřebí předběžná preventivní opatření na ochranu soukromí. Tento princip se týká

g. Řídicích procesů
h. Identifikovatelnosti
i. Tvorby rozsáhlých datových souborů, které dohromady představují mnohem více citlivé osobní údaje, než jednotlivé datové položky samy
j. Přesnosti analýzy, zejména falešně pozitivních a falešně negativních dopadů na jedince
k. Využití analýzy osobních údajů pro osobní řízení rizik v rámci zdravotnictví, financí a mnoha dalších druhů služeb.

6. Anonymity when in public domains should be the norm When in public environments both physical where sensors (including cameras) are used and virtual environments such as multi-player games, or using the web, individuals should be able to expect their identifiability to be limited to those they already know or have agreed to be identified by, otherwise anonymity should be the norm unless national laws require otherwise.	**6. Anonymita, nezbytná norma ve veřejném prostředí** Když ve veřejném prostředí, jak ve fyzickém smyslu (např. použití kamer) i ve virtuální podstatě (jako jsou hry pro více hráčů, nebo prostřednictvím internetu), jednotlivci musí být umožněno předpokládat, že jeho identifikovatelnost je omezena na ty, kteří se již znají, nebo se dohodli na identifikaci; jinak musí být normou anonymita, pokud vnitrostátní právní předpisy nestanoví jinak.
7. Accountability for statements and views made in public In public environments individuals should expect to be held legally accountable for the accuracy of their public statements and any harm caused to others as determined by national laws.	**7. Odpovědnost za prohlášení a názory učiněných na veřejnosti** Ve veřejném prostředí může jednotlivec očekávat, že se bude konat s právní odpovědností a spolehlivostí ohledně správnosti veřejných prohlášení jednotlivce a ohledně jakékoli škody způsobené druhou osobou, jak je stanoveno vnitrostátními právními předpisy.