Za obdelavo osebnih podatkov moramo imeti pravno podlago – možnih je več podlag, a mora ustrezati konkretni situaciji. O obdelavi podatkov moramo informirati posameznika: kdo smo, katere podatke želimo, kaj bomo z njimi počeli, kako dolgo jih bomo hranili, kakšne pravice ima posameznik. Podatke zbiramo in uporabljamo pošteno, ne zbiramo jih na skrivaj, z izsiljevanjem ali zavajanjem.

Če zbiramo in uporabljamo osebne podatke to počnemo z določenimi nameni – ti morajo biti zakoniti. Uporaba podatkov za druge namene brez pravne podlage ni dopustna. Osebnih podatkov ne smemo uporabljati za delanje uslug prijateljem, jih ne preprodajamo in ne »firbcamo« po bazah podatkov iz radovednosti. Če imamo v službi dostop do določenih podatkov, to še ne pomeni, da jih lahko uporabljamo za karkoli.

Nekatere namene lahko dosežemo z anonimnimi podatki in takrat ni potrebno zbirati osebnih podatkov. Če pa brez osebnih podatkov ne gre, zberemo samo tiste podatke, ki so dejansko potrebni, samo od tistih oseb, od katerih jih potrebujemo in takrat, ko so dejansko potrebni. Osebnih podatkov ne zbiramo na zalogo, vnaprej in od vseh in jih ne hranimo v neskončnost.
»~~ker je takšen obrazec~~« »~~nam bodo že prišli prav~~«

VARSTVO OSEBNIH PODATKOV JE V OSNOVI PREPROSTO.

VRTI SE OKROG TEMELJNIH NAČEL VARSTVA OSEBNIH PODATKOV.

6+1 OSNOVIH NAČEL, KI SO DEL VSAKE ZAKONODAJE O VARSTVU OSEBNIH PODATKOV

KO ZMANJKA KONKRETNIH ODGOVOROV, ALI JE NEKAJ PRAV ALI NE, SE VRNEMO K TEMELJNIM NAČELOM.

NAČELO ODGOVORNOSTI

UPRAVLJAVCI IN OBDELOVALCI OSEBNIH PODATKOV MORAJO IZKAZATI, DA RAZUMEJO IN SPOŠTUJEJO TEMELJNA NAČELA VARSTVA OSEBNIH PODATKOV IN SO SPOSOBNI TO TUDI IZKAZATI.

Posamezniki lahko utrpijo resne posledice, če imamo o njih napačne, netočne, nepopolne ali zastarele podatke. Lahko jim je odklonjen kredit, štipendija ali druge pravice, so po krivem obtoženi ali diskriminirani. Pazimo na točnost podatkov pri njihovem vnosu in pri uporabi.

Če smo osebne podatke že zbrali, smo jih zbrali za določene namene. Ko so ti nameni doseženi, moramo podatke uničiti, izbrisati ali jih anonimizirati. Pred tem preverimo, ali nam morda kakšen zakon narekuje daljšo hrambo. Rok hrambe moramo opredeliti še pred samim zbiranjem in z njim tudi seznaniti posameznike.

Zbrane podatke moremo zaščiti pred izgubo, nepooblaščenimi dostopi in spremembami, uničenjem in nedostopnostjo. Informacijsko varnost lahko zagotovimo s kombinacijo organizacijskih in tehničnih ukrepov. Podatki morajo biti na voljo samo pooblaščenim osebam (zaupnost), nedopustno je njihovo nepooblaščeno spreminjanje ali brisanje (celovitost), na voljo morajo biti, ko jih potrebujemo (razpoložljivost).

INFORMACIJSKI POOBLAŠČENEC