

# **HRVATSKO DRUŠTVO ZA MEDICINSKU INFORMATIKU**



**Dokument**

**Načela i smjernice zaštite osobnih podataka**

**Zagreb, 2000**

Dokument: "Načela i smjernice zaštite osobnih podataka" je nastao kao rezultat rada Radne grupe za zaštitu podataka unutar HRVATSKOG DRUŠTVA ZA MEDICINSKU INFORMATIKU. Njegove smjernice predstavljaju konkretne operativne korake, koje bi izvođači zdravstvene djelatnosti mogli rabiti tijekom svojega rada. To znači, da područje zaštite osobnih podataka unutar zdravstvenog informacijskog sustava (ZIS) u Republici Hrvatskoj ne bi više bilo prepušteno vlastitoj volonterskoj inicijativi.

Svi parametri ovoga dokumenta su dinamične kategorije, što znači, da svaki izvođač može prilagoditi dokument svojim potrebama. Međutim, njegova glavna namjena je promjena kulturnih navika u odnosu na uporabu osobnih podataka unutar ZIS-a. Dokument sadrži najnovije materijale na području zaštite osobnih podataka, koji su nastali na tom području unutar Vijeća Europe i Europske Zajednice.

Mladen Markota  
Josipa Kern

Dokument je pripremila projektna skupina HRVATSKOG DRUŠTVA ZA  
MEDICINSKU INFORMATIKU:

Mladen Markota, Josipa Kern, Davor Matić, Dražen Pomper, Josip Duančić

Copyright © 2000, HRVATSKO DRUŠTVO ZA MEDICINSKU INFORMATIKU.  
Sva prava pridržana. Niti jedan dio ovoga Dokumenta se ne može objaviti,  
reproducirati ili nadomjestiti bez odobrenja vlasnika copyrighta – HRVATSKOG  
DRUŠTVA ZA MEDICINSKU INFORMATIKU.

**Nikoga se ne smije uznemiravati samovoljnim miješanjem u njegov privatni život, njegovu obitelj, njegov stan, njegovo privatno dopisivanje ili napadom na njegovu čast i ugled.**

**Opća deklaracija ljudskih prava – 10. Prosinca 1948.**

# 1. UVOD

## 1.1. ZAŠTITA OSOBNIH PODATAKA

Većina odluka koje se repliciraju na pojedinca, u suvremenom društvu temelji se na podacima pohranjenim u automatski vođenim skupovima podataka. Načelo odgovornosti osigurava da na taj način čuvani podaci i njihova uporaba neće posegnuti u pravnu sferu privatnosti pojedinca na kojega se ti podaci odnose.

Problem privatnosti ne izvire samo iz uporabe modernih informacijskih tehnologija. Problem privatnosti je vezan uz sakupljanje, obradu, čuvanje i uporabu osobnih podataka. Moderna tehnologija i uporaba moderne informacijske tehnologije je taj problem samo potencirala, jer kompjutorski potpomognuti skupovi podataka omogućuju brzo udruživanje individualnih osobnih podataka na jednom mjestu i povezivanje datoteka koje se nalaze kod različitih službi.

Privatnost ili pravo na privatnost ima u različitim političkim uređenjima različit sadržaj. Ishodišta za zaštitu osobnih podataka i podataka uopće u zdravstvenim sustavima jesu osnovna ljudska prava, koja su civilizacijska tekovina. Jedna od prvih definicija privatnosti se je oblikovala već krajem prošlog stoljeća u Sjedinjenim Američkim Državama. Po toj definiciji je to pravo pojedinca da ga se pusti na miru (engl. - right to be alone). Za potrebe modernih društvenih sustava kojima osnovu za funkcioniranje predstavljaju upravo informacije, takva definicija ne odgovara u cjelini. Zbog toga se u najnovije vrijeme, pravo na privatnost definira kao pravo pojedinca da zahtijeva, da se podaci koji se odnose na njega ne daju bilo kome.

Ukoliko udružimo potrebu za pravnom zaštitom osobnih podataka sa, za to potrebnim organizacijskim i sigurnosnim mjerama, dolazimo do pojma zaštite osobnih podataka (engl. Data protection). Zaštita osobnih podataka obuhvaća tajnost osobnih podataka (engl. Data privacy), koja je u prvom redu pravno pitanje i sigurnost osobnih podataka (engl. Data security), čiji je cilj fizičko čuvanje opreme kojom se obrađuju osobni podaci, čuvanje prostorija, obrada podataka i komunikacija (1).

U proteklom periodu (zadnjih pet do deset godina) se u procesu srećemo s tradicionalnim arhivskim skupovima podataka i zdravstvenom dokumentacijom koja se čuva isključivo na papiru, (još uvijek predstavlja 70 do 80% svih skupova), ali i sa postupnim uvođenjem novih kompjutorski potpomognutih skupova podataka (1). Neki autori navode tri sastavna dijela privatnosti. Prvi označuju kao privatnost u prostoru i odnosi se na želju pojedinca da ima mogućnosti biti sam tj. odvojen od fizičke prisutnosti drugih osoba. Drugu označuju kao privatnost osobnosti, a odnosi se na slobodu misli, opredjeljenja i izražavanja. Govoreći o privatnosti najčešće upravo mislimo na te dvije komponente, dok se treća - informacijska privatnost (engl. - Information privacy), najčešće zanemaruje. Njena bit je u želji pojedinca da zadrži informacije o sebi, jer ne želi da s njima budu upoznati drugi.

S gledišta prava na informacijsku privatnost važno je misliti na sakupljanje, obradu i prijenos podataka te posebno na njihovu upotrebu. Posljedica pogrešnog postupka na bilo kojem od tih nivoa, je nov sadržaj podatka odnosno mijenjanje sadržaja informacije (1).

U svezi s informacijskom privatnošću se kao temeljno pitanje postavlja definiranje pojma informacije i pojma podatka. Podatak možemo definirati kao činjenicu ili ideju u formaliziraniom obliku, podesnu za komuniciranje i različite operacije. Informacija predstavlja i sadrži značenje koje podatku daje čovjek u određenim okolnostima.

Glede rada UN na području zaštite osobnih podataka, prelomnicu predstavlja godina 1974. Te je godine generalni sekretar UN pripremio cjelovit izvještaj na temu "Ljudska prava i znanstveno tehnološki razvoj" (2). U svojem zaključku izvještaj preporučuje državama, koje još nemaju zakonom uređenu zaštitu osobnih podataka, da takav način reguliranja upotrebe osobnih podataka što prije usvoje. Preporuka generalnog sekretara sadrži također i osnovna načela koje bi članice UN trebale uvažavati pri zakonskom uređivanju zaštite osobnih podataka. To su sljedeća načela:

- načelo određenosti
- načelo obavještavanja i
- načelo pristanka

**Načelo određenosti** kaže da se mogu sakupljati samo oni osobni podaci, koji su nužno potrebni da bi se postigao cilj zbog kojega se sakupljaju.

**Načelo obavještavanja** govori o potrebi da se pojedinca prethodno obavijesti koji se osobni podaci o njemu sakupljaju.

**Načelo pristanka** kaže da se mogu sakupljati samo oni osobni podaci za koje je pojedinac pristao da se sakupljaju.

Na ovom je mjestu važno napomenuti da je prvi nacionalni zakon namijenjen zaštitu osobnih podataka prihvaćen u Švedskoj 1973. godine. To međutim nije bio i općenito prvi zakon, koji je uređivao zaštitu osobnih podataka. Prvi zakon, na nivou njemačke savezne države Hessen je bio donešen 1970. godine. Sjedinjene Američke Države su takav zakon dobile 1974. godine. Glede pravnog uređenja pitanja zaštite osobnih podataka u SAD-ma, postoje određene specifičnosti koje izviru iz posebnosti anglosaksonskog prava.

U Europi je zaštita osobnih podataka zakonom uređena u 21 državi. To su: Austrija, Belgija, Češka, Danska, Finska, Grčka, Island, Irska, Izrael, Italija, Luksemburg, Mađarska, Njemačka, Nizozemska, Norveška, Portugal, Slovenija, Španjolska, Švedska, Švicarska i Velika Britanija.

Samo 6 europskih država je zaštitu osobnih podataka definiralo kao ustavnu kategoriju. To su: Austrija, Nizozemska, Portugal, Slovenija, Španjolska i Švedska. Svim europskim državama koje su zakonom uredile zaštitu osobnih podataka je zajedničko:

1. da zakonom uređuju zaštitu osobnih podataka
2. da različita područja (zdravstvo, školstvo, unutarnje poslove itd.) ne uređuju odvojeno posebnim zakonom, već jedinstveno - jednim zakonom. U svim se slučajevima zakon odnosi, kako na kompjutorsko tako i na ručno vođene skupove.
3. da nude istu zaštitu osobnih podataka svojim i stranim državljanima
4. da zaštita obuhvaća sve segmente upotrebe osobnih podataka (sakupljanje, obrada, čuvanje, prijenos, brisanje itd.)
5. da u zakonu točno definiraju pojmove, kao što su: osobni podatak, evidencija, upravljač skupa itd.
6. da oblikuju organe koji prate položaj na području zaštite osobnih podataka, upozoravaju na nepravilnosti, predlažu mjere itd.
7. da dozvoljavaju i izuzeća od načela i pravila zaštite osobnih podataka, samo u slučajevima određenim zakonom.
8. da osiguravaju javnost rada na području sakupljanja osobnih podataka. To znači da svaki pojedinac može u bilo kojem trenutku dobiti uvid u to, koji se osobni podaci i u kojem obsegu o njemu sakupljaju.
9. da dozvoljavaju slobodan prijenos osobnih podataka preko državnih granica, ali samo u drugu državu koja ima također zakonom uređenu zaštitu osobnih podataka.

Usprkos dosljednom zalaganju za poštivanje prava pojedinca na zaštitu njegovih osobnih podataka, živimo u vremenu u kojem je nemoguće zamisliti, da bi se država odrekla prava da poseže u sferu privatnosti pojedinca. U tu svrhu se zato često spominje tzv. "javni interes", koji u biti predstavlja protutežu za posezanje u područje privatnosti odnosno integriteta pojedinca. Upravo na području osobnih podataka dolazi do suprotnih interesa između države i pojedinca. Za obavljanje nekih funkcija država u prvom redu treba neke podatke, pa i one koji imaju značaj osobnih podataka. To je posebno izraženo na području javne sigurnosti, sprečavanja zaraznih bolesti itd. (1).

## **1.2. DOKUMENTI NA PODRUČJU ZAŠTITE OSOBNIH PODATAKA VIJEĆA EUROPE I EUROPSKE ZAJEDNICE**

### **1.2.1. DOKUMENTI VIJEĆA EUROPE**

U većini država Europske Zajednice postoje posebni zakoni o zaštiti osobnih podataka. Prve preporuke na tom području su nastale u okviru OECD-a i Vijeća Europe u 80-tim godinama ovog stoljeća. Razlog za nastanak tih dokumenata je

bila spoznaja, da masovna obrada osobnih podataka predstavlja objektivnu opasnost za sigurnost informacijske privatnosti pojedinca. S tog aspekta je posebno opasna izuzetno velika sposobnost - kapacitet računalskih sustava, koji omogućuju :

- pohranjivanje enormno velikih količina podataka na relativno malim medijima;
- jednostavnu i brzu reprodukciju sačuvanih podataka i
- lak pristup podacima te jednostavnu promjenu sadržaja sačuvanih podataka

Nova tehnička sredstva su uzrokovala ozbiljnu prijetnju informacijskoj privatnosti pojedinca zbog:

- jednostavnog dobivanja i vođenja podataka, koji nisu neophodno potrebni za obavljanje funkcija određenih organa javne uprave (npr. podaci o osobnom životu pojedinca);
- mogućnosti obrade podataka na način i za namjene, koje nisu bile unaprijed predviđene;
- mogućnosti prijenosa i krađe podataka sačuvanih na nekonvencionalnom mediju
- mogućnosti mijenjanja ili brisanja podataka s magnetnog medija bez posebne punomoći i
- najvažnijeg i najznačajnijeg razloga - mogućnosti sakupljanja i udruživanja podataka različitih skupova podataka čime je moguće sagraditi opsežni skup podataka o osobnom životu pojedinca.

Zbog svega toga su OECD i Vijeće Europe početkom osamdesetih godina predlagali preporuke koje bi u svoje nacionalne zakone ugradile sve članice tih integracija. S tog aspekta je najvažnija:

### **Konvencija Vijeća Europe br. 108. o zaštiti pojedinca glede automatske obrade podataka**

Sa stanovišta međunarodnog prava Konvencije su posebna vrsta međunarodnih ugovora, koji svojim sadržajem obvezuju države potpisnice, da ispune preuzete obveze.

Konvenciju br. 108. je do danas potpisalo i ratificiralo 17 europskih država (tablica 1).

Tablica 1.

država	potpis Konvencije	ratificiranje
Austrija	28.1.1981.	30.3.1988.
Belgija	7.5.1982.	28.5.1993.
Danska	28.1.1981.	23.10.1989.
Finska	10.4.1991.	2.12.1991.
Francuska	28.1.1981.	24.3.1983.
Italija	28.1.1981.	14.6.1997.
Njemačka	28.1.1981.	19.6.1986.
Island	27.9.1982.	25.3.1991.
Irska	18.12.1986.	25.4.1990.
Luksemburg	28.1.1981.	10.2.1988.
Nizozemska	21.1.1988.	24.8.1993.
Norveška	13.3.1981.	20.2.1984.
Portugal	14.5.1981.	2.9.1993.
Slovenija	23.11.1993.	25.1.1994.
Španjolska	28.1.1982.	31.1.1984.
Švedska	28.1.1981.	29.9.1982.
Velika Britanija	14.5.1981.	26.8.1987.

\*Italija je Konvenciju potpisala 1981.godine, ratificirala tek 1997. Zakon o zaštiti osobnih podataka je Italija dobila početkom 1998. godine.

U drugu kategoriju spadaju države koje su Konvenciju potpisale, međutim nisu je još ratificirale (tablica 2.).

Tablica 2.

država	potpis Konvencije	ratifikacija
Cipar	25.7.1986.	/
Grčka	17.2.1983.	/
Mađarska	13.5.1993.	/
Turska	28.1.1981.	/

U treću kategoriju spadaju države koje su članice Vijeća Europe, međutim Konvenciju nisu niti potpisale niti ratificirale. To su:

- Bugarska
- Češka
- Estonija
- Hrvatska
- Litva
- Latvija

- Estonija
- Lichtenstein
- Jalta
- Poljska
- Rumunjska
- Rusija
- San Marino
- Slovačka
- Albanija

Konvencija u 2. članku – točka a) određuje, da osobni podatak predstavlja svaku informaciju, koja se odnosi na određenu ili odredljivu osobu (u engleskom originalu Konvencije: " For the purposes of this Convention 'personal data' means any information relating to an identified or identifiable individual - 'data subject' "). Osnovna dilema koja se je pojavila tijekom interpretacije sadržaja te definicije je: Koliko široko se može tumačiti pojam "osobni podatak", odnosno: da li definicija tog pojma pokriva ili štiti također:

- osobne podatke o umrloj osobi
- osobne podatke nerođenog djeteta
- filmske, fotografske i druge videosnimke fizičke osobe
- glas, odnosno zvučne snimke fizičke osobe

Prevladava stajalište, da se Konvencija br. 108. eksplicitno ne odnosi na podatke o umrloj osobi, ali ujedno i ne isključuje mogućnost interpretacije, da se zaštita proteže i na te podatke. To potvrđuje 11. članak Konvencije koji glasi: "Niti jedna odluka 2. poglavlja se ne može tumačiti tako da bi na bilo koji način onemogućavala članicama potpisnicama, da osiguraju pojedincu na kojega se podaci odnose, širu zaštitu od one koja je dogovorena sa ovom Konvencijom".

Konvencija br. 108. u svojem 5. članku sadrži temeljna načela zaštite osobnih podataka. To su:

- Načelo kakvoće podataka.

Sadrži pet zahtjeva, koje je potrebno uvažavati tijekom automatske obrade podataka. Prvi zahtjeva, da osobni podaci moraju biti dobiveni i obrađeni na zakonit način. Što se računa za zakonit način, ovisi od uređenja u nacionalnom zakonu. Drugi zahtjeva definiranje namjene obrade osobnih podataka. Značajka trećeg zahtjeva je u tome da moraju biti osobni podaci primjereni, relevantni i ne prekomjerni glede namjene zbog koje su bili obrađivani. Četvrti zahtjev se odnosi na točnost podataka. Zadnji, peti zahtjev se odnosi na oblik čuvanja osobnih podataka. Osobni podaci moraju biti sačuvani u obliku, koji omogućuje identifikaciju pojedinca na kojega se odnose samo toliko vremena koliko je potrebno da se postigne namjena zbog kojega su bili sakupljeni.

- Načelo sigurnosti podataka

Obvezuje zemlje potpisnice Konvencije da prihvate odgovarajuće mjere kojim se spriječava slučajno ili neovlašteno uništavanje podataka ili njihov gubitak. Kakve će to biti mjere ovisi o stanju i stupnju razvoja metoda i tehnike na području obrade osobnih podataka u pojedinoj državi – potpisnici Konvencije.

- Načelo otvorenosti

Zahtijeva da svakom pojedincu mora biti omogućeno: da se upozna sa postojanjem automatskog skupa podataka, koji sadrži njegove osobne podatke, njenom namjenom i adresom upravljača skupa.

- Načelo izuzeća

Konvencija dopušta izuzeća od do sada prikazanih načela samo u slučajevima predviđenim u zakonu države potpisnice i uz uvažavanje temeljnih vrednota demokratske države.

- Načelo odgovornosti

Države potpisnice moraju odrediti odgovarajuće sankcije i druga sredstva za primjere kršenja mjera prihvaćenih u okviru nacionalnog zakonodavstva.

U svojem 6. članku Konvencija zabranjuje sakupljanje osobnih podataka koji se odnose na raso podrijetlo, politička, vjerska ili druga uvjerenja, kao i podataka koji se odnose na spolni život pojedinca – ukoliko nacionalno zakonodavstvo ne određuje određenu zaštitu.

U svom 8. članku Konvencija određuje da svakoj osobi mora biti omogućeno :

- da zna za postojanje automatskog skupa osobnih podataka u kojoj su njeni osobni podaci, glavnu namjenu i upravljača tog skupa podataka;
- da dobije u razumnom vremenu potvrdu o tome, koji se osobni podaci sakupljaju o njoj;
- da zahtijeva popravak ili brisanje krivo upisanih osobnih podataka

U okviru Konvencije br. 108 Vijeće Europe je prihvatilo cijeli niz preporuka o zaštiti osobnih podataka na sljedećim područjima: području socijalnog osiguranja, području znanstvenoistraživačkog rada, telekomunikacija, automatskih skupova osobnih podataka na području zdravstva.

Iako se Konvencija prije svega odnosi na osobne podatke koje se vode u automatskom skupu podataka, ona prepušta svakoj državi potpisnici mogućnost da proširi uporabu Konvencije i na skupove podataka koje se vode ručno. Spomenutu mogućnost je iskoristila većina država potpisnica (3).

### **Preporuka broj R(81)1 Komiteta ministara Vijeća Europe o pravilima za automatizirane zbirke podataka, Strassbourg, 1981.**

Načela koje sadrži Preporuka se upotrebljavaju za automatsko vođene skupa podataka unutar sustava zdravstvene zaštite. To su sljedeća načela:

Načelo javnosti – projekti o uspostavi novih medicinskih skupova osobnih podataka moraju prethodno biti predstavljeni javnosti, odnosno javnost mora biti upoznata s njima i to prije svega sa: a) imenom medicinskog skupa podataka, b) namjenom zbog koje se uspostavlja i c) najvažnijim značajkama

Načelo bitnih sadržaja – određuje najvažnije sadržaje pojedine medicinske skupove podatka: a) spisak osobnih podataka koje će se sakupljati, b) navođenje osoba koje imaju pravo upotrebljavati osobne podatke, određenje upravljača zbirke i vrijeme čuvanja osobnih podataka.

Načelo dostupa do osobnih podataka – Izvorno načelo je da pravo pristupa medicinskom skupu osobnih podataka imaju samo zdravstveni radnici u okviru svoje zakonske punomoći ili sa zdravstvenom djelatnošću povezani djelatnici koji trebaju podatke za zadatke ali samo u opsegu u kojem je to potrebno (4).

### **Preporuka broj R(83)10 Komiteta ministara Vijeća Europe o pravilima za automatizirane skupove podataka, Strasbourg, 1983.**

Načela koja sadrži se upotrebljavaju tijekom znanstveno istraživačkog rada bez obzira da li se radi o javnom ili privatnom sektoru.

Načelo privatnosti – mora biti osigurano tijekom svakog istraživačkog projekta.

Načelo anonimnosti – zahtijeva, da kada je to moguće, mora biti istraživanje izvedeno na osnovi anonimnih podataka

Načelo informiranosti – zahtijeva da svaka osoba uključena u istraživanje bude upoznata sa ciljevima istraživanja.

Upravo ta dva načela – načelo anonimnosti i načelo informiranosti su bili povod da je vijeće Europe pristupilo (pod pritiskom zdravstvenog lobija) izradi nove preporuke koja će u nekoj mjeri “liberalizirati” uporabu osobnih podataka za znanstveno istraživačke namjene. Istraživački lobi je tvrdio da načelo anonimnosti implicira slabu kvalitetu sakupljenih podataka i neizvedljivost istraživanja, načelo informiranosti sa druge strane zahtijeva previše vremena (5).

Kao rezultat višegodišnjeg rada stručnjaka Vijeća Europe 1997. godine smo dobili najnoviju preporuku:

## **Preporuka broj R(96) Ministara Vijeća Europe o zaštiti osobnih podataka u sustavu zdravstva**

Radi se o najnovijoj preporuci Vijeća Europe koja definira zaštitu osobnih podataka isključivo u zdravstvu. Njena novost je ta da donosi nove definicije medicinskog i genetskog osobnog podatka, određuje uporabu osobnih podataka umrle osobe, upotrebu genetskih podataka, te uporabu osobnih podataka tijekom znanstveno istraživačkog rada. U tom smislu definira pojam javni interes istraživanja. U svojem 12. članku navodi:

*Uvijek kada je to moguće osobni podaci za znanstvenoistraživački rad trebali bi biti anonimni.*

Kada ta anonimnost implicira neizvedivost istraživanja, istraživanje se može nastaviti ukoliko:

- se subjekt podatka izričito ne protivi uporabi istih
- uporaba osobnih podataka implicira javni interes istraživanja
- je subjekt podatka dao pismenu suglasnost

U svakom slučaju javni interes također mora biti zakonski određen zakonom, koji govori o uporabi osobnih podataka unutar zdravstvenog sustava ili kroz neki drugi statistički zakon (6).

### **1.2.2. DOKUMENTI EUROPSKE ZAJEDNICE**

#### **Direktiva 95/46/EC Europskog Parlamenta i Savjeta**

Prijedlog Direktive je bio oblikovan tijekom 1990. godine na osnovu načela zaštite prava i sloboda, koje sadrži Konvencija br. 108. Vijeća Europe od 28. siječnja 1981. godine (7). Pojedine zahtjeve iz petoga člana Konvencije br. 108. je Direktiva podigla na nivo načela. Direktiva je zanimljiva iz dva razloga:

Prvi je, da se radi o najnovijem dokumentu na području reguliranja zaštite osobnih podataka u vidu jednog od većih međunarodnih integrativnih oblika, čija načela moraju biti uključena u nacionalne zakone svih članica Europske zajednice do 24. kolovoza 1998. godine.

Drugi je taj, da postavlja pravila za sve koji jesu i koji žele postati članice Zajednice. Načela sadržana u direktivi se mogu dopuniti za određene sustave posebnim pravilima, koja se moraju temeljiti na tim načelima. S obzirom na podjelu na javni i privatni sektor, načela sadržana u direktivi možemo podijeliti u tri grupe:

- Načela zaštite osobnih podataka u javnom sektoru
- Načela zaštite osobnih podataka u privatnom sektoru
- Načela koja su zajednička javnom i privatnom sektoru

## **Načela zaštite osobnih podataka u javnom sektoru**

### **• načelo poštenja i zakonitosti**

Načelo poštenja i zakonitosti zahtijeva da osobni podaci moraju biti obrađeni na pošten i zakonit način, sakupljeni za određene - zakonom odobrene namjene. Podaci moraju biti točni i ažurni. Potrebno je uvijek omogućiti da se netočni ili nepotpuni podaci, s obzirom na cilj zbog kojega su bili sakupljeni, poprave ili izbrišu. Podaci se trebaju čuvati u obliku, koji omogućuje identifikaciju pojedinca toliko vremena, koliko je potrebno da se ostvari cilj, zbog kojega su bili sakupljeni. S tim u svezi države članice EZ moraju osigurati jamstvo za one osobne podatke, koji se čuvaju za povijesnu, statističku ili znanstvenu upotrebu.

### **• načelo prethodnog određivanja namjene sakupljanja**

Države članice moraju osigurati, da se osobni podaci mogu obrađivati samo ukoliko je subjekt podatka nesumnjivo dao svoj pristanak ili je obrada i upotreba podataka potrebna za izvođenje zadatka, u javnom interesu. U tom slučaju taj javni interes mora biti definiran kroz poseban zakon - "lex specialis" (npr. kroz zakon o evidencijama u zdravstvu, školstvu itd.).

### **• načelo restriktivnosti pri razmjeni podataka**

Razmjena osobnih podataka je moguća samo ukoliko pravna ili fizička osoba "iskaže" legitiman interes, pod uvjetom da interes subjekta nije jači.

### **• načelo obavezne prijave**

Načelo zahtijeva, da mora biti proces uspostavljanja skupova osobnih podataka prethodno prijavljen nadzornom državnom organu i registriran u katalogu-registru skupova, koji sadrže osobne podatke. Katalog ili registar moraju biti javni.

## **Načela zaštite osobnih podataka u privatnom sektoru**

Načela, koja po prijedlogu Direktive moraju biti ispunjena za zakonito sakupljanje osobnih podataka u privatnom sektoru su identična načelima, koja vrijede u javnom sektoru, sa razlikom da je njihov sadržaj prilagođen odnosu između pojedinca i subjekta privatnog sektora.

## **Načela koja su zajednička javnom i privatnom sektoru**

### **• načelo notifikacije**

Načelo je uvjet za valjanost pristanka pojedinca, da se njegovi osobni podaci sakupljaju. Takav pristanak vrijedio bi jedino u slučaju kada:

a) subjekt dobije prethodno sljedeće informacije:

- informaciju o imenu i adresi upravljača skupa
- informaciju o namjeni i sadržaju skupa

b) subjekt svoj pristanak povuče u bilo kojem trenutku

U okvir načela notifikacije spada i pravo pojedinca na kojega se podaci odnose, da tijekom sakupljanja tih podataka bude obaviješten o:

- imenu i adresi upravitelja skupa
- posljedicama ukoliko ne da podatke
- tome kome će se podaci slati
- mogućnosti popravka podataka

### **• načelo sudjelovanja pojedinca**

Pojedincu, na kojega se odnose osobni podaci, mora biti osigurano:

- da se ne slaže s procesiranjem osobnih podataka, ukoliko ima za to legitimne razloge
- da neće biti podvrgnut administrativnim odlukama, kada mu se tim odlukama poseže u njegova prava, a kada se te odluke temelje na slici, koja je bila ostvarena isključivo na osnovu automatskog procesiranja podataka.
- da dobije u razumnom vremenu i bez velikih troškova potvrdu o tome da li su u određenom skupu sačuvani podaci o njemu i po potrebi ispis tih podataka u razumljivom obliku.
- da zahtjeva popravak, brisanje ili blokiranje podataka, ukoliko su bili procesirani u suprotnosti sa načelima Direktive.
- da zahtijeva da se druge osobe, kojima su već bili poslani podaci, obavijesti o popravku, brisanju ili blokiranju podataka.

### **• načelo restriktivnosti**

Određuje da je moguće ograničiti prava pojedinca, na kojega se osobni podaci odnose, samo ukoliko to određuju razlozi nacionalne sigurnosti, obrane, krivičnog gonjenja, javne sigurnosti, ekonomski i financijski interesi države ili izvršavanje nadzornih i inspeksijskih zadataka države.

### **• načelo zakonitosti**

Identično je načelima zakonitosti, koje vrijede za načela u javnom sektoru.

### **• načelo zabrane**

Članice moraju zabraniti obradu osobnih podataka, koji se odnose na vjersku, rasnu ili etničku pripadnost, politička uvjerenja, filozofska stajališta, članstvo u sindikatu i podatke o zdravlju ili spolnom životu. Iznimku predstavlja pristanak

subjekta za sakupljanje takvih podataka. Samo zakon može odrediti iznimke toga načela i to za određene podatke i za točno definirane korisnike.

• **načelo osiguranja**

Načelo obvezuje prihvaćanje određenih organizacijskih i tehničkih mjera za zaštitu osobnih podataka pred slučajnim ili neovlaštenim uništenjem, promjenom sadržaja ili gubitkom.

Među dokumentima Vijeća Europe i Europske Unije, dva zaslužuju posebnu pažnju. To su: Konvencija br. 108. koja predstavlja ishodište za sve ostale dokumente na području ZOP i Direktiva Europske Unije čije se odredbe moraju uključiti u nacionalne zakone pojedinih članica do 24 kolovoza 1998. Odnos između ta dva dokumenta prikazuje tablica 3.

Tablica 3. Odnos između Konvencije br. 108. Vijeća Europe i Direktive EU

<b>Odredba Konvencije br.108</b>	<b>Odredba Direktive EU</b>	<b>Zaključak</b>
Opseg zaštite osobnih podataka:  - vrijedi za skupove osobnih podataka, koje se vode sredstvima automatske obrade podataka (1. i 3 članak)	Opseg zaštite osobnih podataka:  - vrijedi za skupove osobnih podataka, koje se vode sredstvima automatske obrade podataka ali i za oni skupovi koje su ručno vođene (1. i 3. članak)	Domet Direktive je u odnosu na opseg zaštite veći.
Pravna osnova za obradu osobnih podataka:  - Osobni podaci se obrađuju samo na osnovi zakona (2. članak)	Pravna osnova za obradu osobnih podataka:  - Osobni podaci se obrađuju na osnovi zakona i pismene suglasnosti pojedinca na kojega se podaci odnose (2.,4. i 7. članak)	Direktiva šire određuje pravnu osnovu za obradu osobnih podataka.
Osjetljivi osobni podaci: - Osjetljivi osobni podaci kao što su: etničko podrijetlo, politička pripadnost, seksualni život itd. se mogu obrađivati samo ukoliko za to postoji zakonska osnova ili pisma suglasnost osobe na koju se ti podaci odnose (6. članak)	Osjetljivi osobni podaci: - Osjetljivi osobni podaci kao što su. etničko podrijetlo, politička pripadnost, seksualni život itd. se mogu obrađivati samo ukoliko nacionalni zakon osigurava zaštitu takvih podataka (8. članak)	Obzirom, da sve više zemalja definira zaštitu osobnih podataka i kao ustavnu kategoriju, prevladava stav da je sakupljanje takvih podataka vezano na pismenu suglasnost osobe, na koju se ti podaci odnose.

Tablica 3. Odnos između Konvencije br. 108. Vijeća Europe i Direktive EU (nastavak)

Odredba Konvencije br.108	Odredba Direktive EU	Zaključak
<p>Namjena: - Osobni podaci se čuvaju na osnovu određene zakonske namjene (5. članak)</p>	<p>Namjena: - Osobni podaci se sakupljaju za određenu i zakonom određenu namjenu (6. članak)</p>	<p>Radi se o terminološkim zanimljivostima. Dok Konvencija namjenu veže uz čuvanje osobnih podataka, Direktiva veže namjenu uz sakupljanje</p>
<p>Načelo dostupa do podataka: - Svakoj osobi mora biti omogućeno da bude upoznata s postojanjem automatski skupovi podataka (8. članak)</p>	<p>Načelo dostupa do podataka: - Svatko ima pravo dostupa do osobnih podataka, koji se na njega odnose (12 članak) - Ovlašteni javnopravni organ je odgovoran za notifikaciju skupova osobnih podataka. Sadržaj notifikacije je: naziv i adresa upravljača skupa, namjena sakupljanja, korisnike podataka itd (19. članak) - Dužnost država članica je da vode registar skupova osobnih podataka (14. članak)</p>	<p>Direktiva je u odnosu na Konvenciju obsežnija glede tog pitanja.</p>
<p>Dužnost upravljača skupa: - Svakoj osobi mora biti omogućeno, da zahtijeva popravak ili brisanje osobnih podataka, koji su bili sakupljeni u suprotnosti sa propisima (8. članak)</p>	<p>Dužnost upravljača skupa: Svaki pojedinac ima pravo da se usprotivi obradi njegovih osobnih podataka, ukoliko za to nema zakonske osnove (14. Članak) - Svaka osoba ima pravo na pravednu odštetu u slučaju štete koju joj je nanijelo sakupljanje osobnih podataka, u suprotnosti sa zakonskim osnovama (24. članak)</p>	<p>I na ovom području je Direktiva obsežnija i preciznija u odnosu na Konvenciju.</p>

Na području bolesnikovih prava i području čuvanja osobnih podataka nema značajnih razlika između odredbi Konvencije i odredbi Direktive.

Temeljna razlika između Konvencije i Direktive je u njihovim ciljevima. Dok je temeljni cilj Konvencije zaštita osobnih podataka kao temeljnog ljudskog prava, glavni cilj Direktive je omogućiti cirkulaciju podataka između država članica zbog ekonomskog interesa grupacije.

Druga temeljna razlika je u tome da je Konvencija br. 108 u biti minimalni standard na području zaštite osobnih podataka, Direktiva predstavlja maksimum pravne zaštite na tom području (8,9).

### **1.2.3. OSTALI DOKUMENTI NA PODRUČJU ZAŠTITE OSOBNIH PODATAKA**

#### **Hipokratova zakletva**

„Šutjet ću o svemu, što tijekom vršenja moje dužnosti ili izvanj nje, vidim ili čujem o životu i ponašanju ljudi, jer sam mišljenja da takve podatke trebam čuvati samo za sebe, kao profesionalnu tajnu“.

Hipokratova zakletva je glede zaštite osobnih podataka sveobuhvatna i bez ikakve sumnje obvezujuća. Svakako ona ne daje točnije smjernice o mogućim mjerama zaštite podataka (10).

#### **Ženevska liječnička zakletva**

„Tajne koje su mi povjerene čuvat ću i poslije bolesnikove smrti.“

Zakletva zahtijeva isti odnos prema podacima i poslije bolesnikove smrti. To svakako implicira posebne mjere zaštite osobnih podataka u arhivima bez obzira na medij. Zakletva ne daje smjernice glede trajanja čuvanja pojedinih podataka (10).

#### **Međunarodni kodeks liječničke etike**

Opće dužnosti liječnika: „Liječnik treba poštivati prava bolesnika, svojih kolega i drugog zdravstvenog osoblja i čuvati povjerljivost podataka o bolesniku.“

Radi se o sveobuhvatnoj obvezi liječnika u odnosu na zaštitu podataka bez obzira na vrstu podataka i vremenski rok (10).

#### **Rezolucija o upotrebi kompjutora u medicini (1973, 1983)**

- Svjetska Zdravstvena Organizacija konstatira veliki napredak i korist koji izvire iz uporabe kompjutora i elektroničke obrade podataka na području zdravstva, prije svega pri njezi bolesnika i u epidemiologiji.
- Nacionalne liječničke udruge moraju prihvatiti sve potrebne mjere da osiguraju tajnost, sigurnost i povjerljivost podataka o svojim bolesnicima.

Rezolucija podupire uporabu moderne informacijske tehnologije u zdravstvu, ali ujedno i predlaže osnovne smjernice na području zaštite osobnih podataka (10).

### **Deklaracija iz Lisabona o pravima bolesnika**

„Bolesnik ima pravo da zahtijeva da liječnik poštuje i čuva tajnost svih njegovih medicinskih i ostalih podataka.“

Deklaracija obvezuje liječnika na isti odnos prema osobnim i neosobnim podacima (11).

### **Opća deklaracija ljudskih prava OZN**

„Nikoga se ne smije uznemiravati samovoljnim miješanjem u njegov privatni život, njegovu obitelj, njegov stan, njegovo privatno dopisivanje ili napadom na njegovu čast i ugled.“ (12)

## **1.3. ZAŠTITA OSOBNIH PODATAKA U POJEDINIM DRŽAVAMA EUROPSKE ZAJEDNICE**

U velikom broju država članica Europske zajednice postoje posebni zakoni o zaštiti osobnih podataka. Prve preporuke na tom području su nastale u okviru OECD-a i Vijeća Europe početkom osamdesetih godina. OECD i Vijeće Europe su predlagali preporuke, koje bi države članice tih integracija morale ugraditi u svoje nacionalno zakonodavstvo. Od godine 1970. nadalje su mnoge europske države prihvatile posebne zakone o zaštiti osobnih podataka. Iznimka su Italija i Grčka, koje još uvijek nemaju prihvaćenog zakona o zaštiti osobnih podataka. Belgija i Španjolska imaju područje zaštite osobnih podataka uređeno u svojim statističkim zakonima. U većini europskih država su oblikovana posebna javnopravna tijela, koja brinu za realizaciju načela i propisa. I u ovom slučaju su Italija i Grčka iznimke (1).

### **Belgija**

Zakon je dobila 1983 godine. Uveo ga je poseban savjetodavni odbor (a Consultative Commission), koji na zahtjev ministra za pravosuđe sastavlja izvještaje o pitanjima, koja se odnose na zaštitu osobnih podataka.

### **Danska**

Radi se o državi sa najdužom tradicijom osobnih identifikacijskih brojeva. Tijekom 1968. i 1977. godine su bile u Danskoj oblikovana tri različita identifikacijska broja koji se upotrebljavaju u javnim skupovima podataka. Zakon o zaštiti osobnih podataka Danska je dobila 1978. tada je bio uspostavljen i nadzorni organ (Data Surveillance Authority). Njegova osnovna funkcija je izrada točnih naputaka za djelovanje i uporabu skupova osobnih podataka i izrada naputaka za zaštitu osobnih podataka.

### **Francuska**

Zakonom o zaštiti osobnih podataka iz godine 1978. je bila uspostavljena Nacionalna komisija za slobode pojedinca i obradu njegovih podataka (Commission Nationale de l'Informatique et des Libertés). Važna zadaća te

komisije je obavještavanje građana o njihovim pravima i obvezama na području sakupljanja, obrade, čuvanja i posredovanja osobnih podataka. Komisiju sastavlja sedamnaest članova za period od pet godina.

#### Irska

Zakonom iz godine 1983. je ustanovila komesara za zaštitu osobnih podataka.

#### Luksemburg

Ima zakon od godine 1979. Na njegovoj osnovi imenuje se poseban odbor pravnika i eksperata na području informatike. Za tu je državu zanimljiva činjenica da vlada nikada ne ignorira savjetodavnu funkciju toga organa.

#### Nizozemska

Zakonom iz godine 1988. je bio uspostavljen registar skupova osobnih podataka na nacionalnom nivou.

#### Njemačka

Njezina savezna država Heslen je dobila prvi zakon o zaštiti osobnih podataka već tijekom 1972 godine. Na cjelovitom saveznom nivou djeluje savezni komesar za zaštitu osobnih podataka (Bundesbeauftragter für den Datenschutz). Pored saveznog u Njemačkoj postoje i komesari na nivou svake pojedine savezne države.

#### Portugal

Značajka zakona o zaštiti osobnih podataka iz godine 1985. je ta, da je uspostavio nacionalnu komisiju koja je jedina nadležna, da odobrava međusobno povezivanje skupova osobnih podataka.

#### Velika Britanija

Zakonom iz godine 1984. je uspostavljen registarski organ (A Data Protection Registrar), u kojeg se moraju registrirati sve zbirke osobnih podataka.

Ishodište za zaštitu osobnih podataka i podataka uopće u sustavu zdravstvene zaštite je u temeljnim ljudskim pravima, koja su civilizacijsko nasljeđe. Zaštita osobnih podataka se odnosi na zaštitu integriteta pojedinca u smislu njegovog prava na informacijsku privatnost. Pri tom je potrebno uvažavati opće prihvaćeno načelo, da su osobni podaci isključivo vlasništvo pojedinca na kojega se odnose.

Osobni podaci će biti sve zanimljiviji za različite subjekte. Zato će i "pritisak" na te podatke postajati sve jači – i na ovlaštene upravljače pojedinim skupovima podataka. S jedne strane mora se osigurati mogućnost bilježenja relevantnih podataka i njihovu dohvatljivost, dakle i mogućnost identifikacije pojedinca radi pružanja primjerene i pravovremene zdravstvene zaštite, a s druge strane svaki pojedinac ima pravo na privatnost, pravo da podaci osjetljive prirode ne budu na dohvat onome tko za to nije ovlašten.

Zbog toga je vrlo važan odnos prema zaštiti osobnih podataka u skladu s načelima i smjernicama o zaštiti osobnih podataka koje su dali relevantni subjekti (VE, EZ itd.). Svaka zemlja treba graditi vlastiti dokument o zaštiti osobnih podataka u zdravstvenom informacijskom sustavu.

U ovom dokumentu upotrijebljeni izrazi znače sljedeće:

1. Podatak

Podatak znači zapis o pojavi, koja je zabilježena u obliku koji omogućuje pored klasične, automatsku obradu pomoću opreme, u skladu sa uputama za postizanje određenog cilja.

2. Osobni podatak

Osobni podatak je podatak koji govori o osobini, stanju ili prilikama pojedinca, bez obzira na oblik u kojem je iskazan. Predmet zaštite su svi osobni podaci.

3. Obrada osobnih podataka

Obrada osobnih podataka predstavlja bilo koju operaciju ili vrstu operacije, koja se odnosi na osobne podatke sa ili bez automatskih pomagala. U obradu spadaju sakupljanje, pohranjivanje, organiziranje, čuvanje, prenašanje, brisanje ili uništavanje osobnih podataka.

4. Zdravstveni podatak

Zdravstveni podatak je svaki osobni podatak, koji govori o zdravstvenom stanju pojedinca.

5. Subjekt podatka

Subjekt podatka je određena ili odredljiva fizička osoba, na koju se odnosi osobni podatak.

6. Pristanak subjekta podatka

Pristanak subjekta podataka znači svaku dragovoljno danu indicaciju želja, s kojom subjekt podataka označi pristanak na obradu osobnih podataka, koji se odnose na njega.

7. Korisnik osobnih podataka

Korisnik osobnih podataka je subjekt, koji je zakonom ili pismenom dozvolom pojedinca ovlašten da upotrebljava osobni podatak.

8. Treća strana

Predstavlja fizičku ili pravnu osobu, javni ured, agenciju ili bilo koji drugi organ, kojega je upravljač osobnih podataka opunomoćio da obrađuje osobne podatke.

## 9. Sigurnost informacijskog sustava

Sigurnost informacijskog sustava obuhvaća:

- povjerljivost podataka, sprečavanje neopunomoćenih osoba da pristupe osobnim podacima
- cjelovitost podataka, sprečavanje neovlaštene promjene ili uništenja osobnih podataka
- raspoložljivost, omogućavanje ovlaštenim osobama konstantan pristup do skupu osobnih podataka.

## 10. Upravljač osobnih podataka

Upravljač osobnih podataka je subjekt, koji je zakonom ili na osnovu pismene suglasnosti pojedinca, na kojega se osobni podaci odnose ovlašten da uspostavi, vodi, održava i nadzire skup osobnih podataka i u tu svrhu sakuplja, obrađuje, čuva i razmjenjuje osobne podatke.

## 11. Nadzorni organ

Nadzorni organ je fizička ili pravna osoba, javni ured, agencija ili bilo koji drugi organ, koji sam ili zajedno sa nekim drugim određuje namjene i sredstva za obradu osobnih podataka.

## 12. Osigurani prostor

Osigurani prostor su sve prostorije u kojima je strojna i programska oprema koja sadrži osobne podatke te svi ostali prostori u kojima se nalaze skupovi osobnih podataka vođene na klasičan način.

## 13. Strojna oprema

Strojna oprema je oprema za unos, obradu, prikaz, čuvanje i posredovanje podataka.

## 14. Programska oprema

Programsku opremu čine kompjutorski programi:

- a) sistemski – programi za upravljanje strojnom opremom i komuniciranje okolinom i oprema koja je namijenjena razvoju aplikacijskih programa.
- b) aplikativni – programi sa kojima se izvodi obrada podataka sa svrhom da se dobiju informacije potrebne korisniku.

## 15. HCE

Engleski izraz za Health Care Establishment. Predstavlja vodstvo zdravstvene ustanove.

## 16. Kriptografija

Kriptografija je matematička znanost o skrivanju poruka.

## **2. DOKUMENT – NAČELA I SMJERNICE ZAŠTITE OSOBNIH PODATAKA U ZDRAVSTVENOM INFORMACIJSKOM SUSTAVU**

Zaštita osobnih podataka obuhvaća tajnost osobnih podataka (Data privacy), koja je u prvom redu pravno pitanje i sigurnost osobnih podataka. Odnosi se na čuvanje integriteta pojedinca u smislu njegovog prava na informacijsku privatnost. (Data security), čiji je cilj fizičko čuvanje opreme kojom se obrađuju osobni podaci, prostorija, obrada podataka i komunikacija njima.

U skladu za rezultatima analize stavova ispitivanih liječnika prijedlog dokumenta sadrži načela i smjernice koje bi tijekom svoga rada mogli upotrebljavali liječnici bez obzira na djelatnost.

Potpuna zaštita osobnih podataka nije moguća. Uporaba moderne informacijske tehnologije taj problem samo potencira odnosno ponovno osvjetljava (15).

Svi parametri dokumenta su dinamične kategorije. Njegova glavna namjena je promjena navika i kulture ponašanja korisnika osobnih podataka.

Dokument sadrži načela zaštite osobnih podataka glede sektora djelatnosti. Svakom načelu je priključen određeni broj smjernica koje predstavljaju konkretne operativne korake koje trebaju uvažiti izvođači unutar zdravstvene djelatnosti. Dokument uključuje sva najnovija dostignuća na području zaštite osobnih podataka unutar Vijeća Europe i Europske Zajednice objavljena do godine 1997. (3, 4, 5, 6, 7,16).

Analiza odgovora je pokazala da su liječnici različitih djelatnosti različito upoznati sa zakonskim osnovama. Za mlađe liječnike zaštita osobnih podataka ne predstavlja važno područje u njihovom svakidašnjem radu. Također su najmanje upoznati sa zakonskim osnovama i ostalim dokumentima, koji reguliraju to područje. Vrlo su tolerantni prema uporabi njihovih osobnih podataka u drugim sustavima.

Mnogi liječnici misle da se zdravstvena dokumentacija u njihovoj ustanovi slabo čuva. "Password" se pretežno ne upotrebljava i prevelik je broj onih liječnika koji se slažu s općom dostupnošću osobnim podacima svim zaposlenima. Rezultati ankete i činjenica da većina "napada" na sigurnost sustava računa na nepoštivanje i neuvažavanje osnovnih i najjednostavnijih sigurnosnih pravila i ne kako se često misli na "slom" sustava zaštite koji se temelji na sofisticiranim mjerama zaštite (asimetrična kriptografija i dr.) (17,18).

Zbog toga dokument posebnu pažnju posvećuje području naobrazbe i sigurnosnim mjerama zaštite osobnih podataka.

U skladu sa najnovijom Direktivom 95/46/EC Europskog Parlamenta i Savjeta (7) (odredbe Direktive su morale biti uključene u nacionalne zakone svih članica Europske Zajednice do 24. kolovoza 1998) (9) načela moramo podijeliti u tri grupe:

1. Načela i smjernice zaštite osobnih podataka u javnom sektoru
2. Načela i smjernice zaštite osobnih podataka u privatnom sektoru
3. Načela i smjernice zaštite osobnih podataka koja su zajednička javnom i privatnom sektoru

Po prijedlogu Direktive u "javni sektor" spadaju sve organizacije i tijela u državama članicama, koje spadaju pod režim javnog prava (Public Law).

U "privatni sektor" (Private sector) spadaju sve fizičke osobe, pravne osobe ili udruženja, uključujući i subjekte javnog sektora, ukoliko se bave privrednom i trgovačkom djelatnosti (7).

### ***Načela i smjernice zaštite osobnih podataka u javnom sektoru***

#### **1. Načelo zakonitosti**

Načelo zakonitosti zahtijeva zakonitost tijekom uspostave skupa osobnih podataka. Osobni podaci moraju biti sakupljeni i obrađeni na pošten i zakonit način, sačuvani za zakonom točno određenu namjenu i upotrijebljeni na način koji je u skladu sa tom namjenom

*Smjernica 1.* Svi medicinski skupovi podataka (MSP) uspostavljeni na temelju zakona a koji sadrže osobne podatke moraju definirati: namjenu MSP, vrstu podataka sadržanih u MSP, fizičke i pravne osobe koje imaju pravo dostupa do MSP, upravljača MSP, vrijeme čuvanja osobnih podataka i uvjete pod kojima je dopušteno povezivanje MSP sa drugim skupovima.

*Smjernica 2.* Pristup osobnim podacima, koje sadrži MSP, imaju samo zdravstveni djelatnici u okviru svojih zakonskih ovlaštenja ili sa zdravstvenom djelatnošću povezani djelatnici, koji trebaju osobne podatke za izvršavanje svojih zadataka

*Smjernica.3.* Zdravstveni djelatnici ili sa zdravstvenom djelatnošću povezani djelatnici moraju čuvati osobne podatke u skladu s zakonskim i etičkim normama.

## **2. Načelo restriktivnosti**

Odnosi se na restriktivnost tijekom razmjene osobnih podataka. Načelno je razmjena osobnih podataka moguće jedino ukoliko fizička ili pravna osoba iskaže legitiman interes za dobivanje osobnih podataka.

*Smjernica 1.* Subjekt podataka bi trebao biti obaviješten o obradi njegovih osobnih podataka i njihovom pošiljanju korisnicima.

*Smjernica 2.* Osobni podaci sadržani u medicinskom skupu podataka načelno se ne bi smjeli razmjenjivati za druge namjene osim u primjeru kada se ta razmjena izvodi u korist bolesnika, kao npr. za potrebe dijagnostike i zdravstvenih usluga, upisivanje podataka u osnovnu medicinsku dokumentaciju, osiguravanje socijalne zaštite (invalidska komisija, liječnički konzilij) itd.

*Smjernica 3.* Razmjena osobnih podataka mora teći u skladu s kodeksom medicinske informatike.

*Smjernica 4.* U slučaju sumnje na nekorektnu upotrebu osobnih podataka od strane korisnika osobnih podataka vodstvo javne zdravstvene ustanove bi trebalo uskratiti njihovu razmjenu i o tome obavijestiti odgovorni nadzorni organ.

*Smjernica 5.* Za znanstveno istraživačke radove može upravljач skupa medicinskih podataka razmijeniti zahtjevano osobne podatke u obliku koji ne omogućuje identifikaciju pojedinca.

*Smjernica 6.* Da bi bilo omogućeno posredovanje osobnih podataka drugim korisnicima mora se osigurati odvojenost:

- podataka koji su administrativne prirode
- podataka koji su medicinske prirode
- podataka koji su socijalne prirode

## **3. Načelo ugovornog odnosa**

Jedan od osnovnih elemenata organizacije ZOP, bez kojega nema niti zaštite podataka je razumljiva i pravilna podjela dužnosti i odgovornosti. Dužnost i odgovornost svih zaposlenih, koji rade sa osobnim podacima moraju biti određeni ugovorom.

*Smjernica 1.* Osobe koje obavljaju javnu službu trebale bi biti formalno i u pismenom obliku upoznate sa svojom odgovornošću. Preporučljivo je da se taj odnos regulira tijekom potpisivanja ugovora o zaposlenju u obliku i na način koji će biti razumljiv za oba partnera.

*Smjernica 2.* Odredbu o sigurnoj i poštenoj obradi osobnih podataka bi trebali sadržavati i ugovori sa vanjskim suradnicima, nabavljačima opreme itd. (treća strana).

*Smjernica 3.* Vodstvo javne zdravstvene ustanove bi trebalo za sve djelatnike pravilnikom točno definirati obveze i zadatke na području zaštite osobnih podataka u obliku pravilnika. Pravilnik o zaštiti osobnih podataka izdaje direktor zdravstvene ustanove.

*Smjernica 4.* Svi djelatnici bi trebali biti upoznati sa sadržajem pravilnika.

*Smjernica 5.* Svi djelatnici bi trebali izvještavati vodstvo zdravstvene ustanove o kršenju i nepravilnostima za koje znaju da postoje.

#### **4. Načelo naobrazbe**

Načelo naglašava važnost naobrazbe i svjesnosti o važnosti zaštite osobnih podataka među zaposlenima u javnom zdravstvenom zavodu.

*Smjernica 1.* Vodstvo javne zdravstvene ustanove bi trebalo biti odgovorno za stalni proces naobrazbe svojih djelatnika na području zaštite osobnih podataka.

*Smjernica 2.* Vodstvo javne zdravstvene ustanove bi trebalo odrediti grupe (bolesnici, njihova rodbina, studenti medicine itd.) koji moraju biti informirani o važnosti zaštite osobnih podataka.

### ***Načela i smjernice zaštite osobnih podataka koja vrijede u javnom i privatnom sektoru***

#### **1. Načelo kodeksa medicinske informatike**

Društvo medicinskih informatičara bi moralo izraditi kodeks medicinske informatike.

*Smjernica 1.* Osnivač kodeksa bi morao posvetiti posebnu pažnju uzvišenosti ideje osobnih prava.

*Smjernica 2.* Sva vodstva zdravstvenih ustanova bi morala uvažavati kodeks medicinske informatike.

## **2. Načelo prava bolesnika**

*Smjernica 1.* Svaki pojedinac se može protiviti obradi njegovih osobnih podataka. Pri tom mora biti svjestan da uporaba osobnih podataka može biti uvjet za pružanje zdravstvene usluge i nuđenje zdravstvene pomoći.

*Smjernica 2.* Ukoliko zakon ne određuje drugačije, osobni podaci bi se smjeli sakupljati isključivo na osnovu pristanka subjekta podataka na kojega se osobni podaci odnose.

*Smjernica 3.* Pristanak subjekta podatka na obradu njegovih osobnih podataka je vjerodostojna jedino ukoliko je pojedinac prethodno bio obaviješten o namjeni MSP koji sadrži njegove osobne podatke, korisnicima MSP i imenu i adresi upravljača skupa podataka.

*Smjernica 4.* Pojedinac bi morao biti obaviješten o tome, da će se njegovi osobni podaci sakupljati, obrađivati i posredovati.

*Smjernica 5.* Pojedinac bi trebalo biti omogućen popravak krivo upisanih osobnih podataka.

*Smjernica 6.* Trošak popravke krivo upisanih osobnih podataka bi trebao snositi upravljač medicinskog skupa podataka.

## **3. Načelo kakvoće MSP**

Osobni podaci bi se morali obrađivati na način koji omogućuje visok nivo kakvoće, točnosti i cjelovitosti.

*Smjernica 1.* Medicinski skup podataka bi trebao biti točan i ažuran.

*Smjernica 2.* Definirani bi trebali biti kriteriji na osnovi kojih je moguće osigurati vrednovanje upotrijebljene programske opreme.

## **4. Načelo mjera sigurnosti**

Određene mjere na području sigurnosti imaju za cilj: sprečavanje neovlaštenog dostupa, sprečavanje uništenja i sprečavanje promjene sadržaja.

*Smjernica 1.* Prostor gdje se nalazi medicinski skup podataka bi trebao biti zaštićeni sistemima tehničke zaštite kao npr. solidne brave, čvrsta vrata, rešetke na prozorima, čelične kase itd.

*Smjernica 2.* Svaki zdravstveni djelatnik bi trebao imati dostup samo do onih podataka, koje stvarno treba tijekom svojega rada. Korisnicima osobnih podataka s obzirom na njihovu djelatnost i profesiju, treba definirati i sastaviti spisak računskih operacija koje su im na raspolaganju po načelu "svatko neka upotrebljava one dijelove programa, koje stvarno treba tijekom svojega rada".

*Smjernica 3.* Sustav bi morao zabilježiti svaki dostup do MSP odnosno zabilježiti svaki događaj koji je zanimljiv sa stanovišta ZOP (datum i vrijeme dostupa, identifikaciju korisnika, tip postupka i vrstu osobnih podataka koje se obrađuju u sistemu).

*Smjernica 4.* Sustav ne bi smio početi s radom dok se korisnik ne identificira.

*Smjernica 5.* Sustav bi morao omogućiti ograničen dostup do medicinskog skupa podataka.

*Smjernica 6.* Ukoliko korisnik duže vrijeme ne upotrebljava sustav, isti bi se morao po određenom vremenu automatski isključiti i o tome upozoriti korisnika

*Smjernica 7.* Protiv virusnu zaštitu trebaju predstavljati organizacijske mjere i tzv. Protiv virusni programi.

*Smjernica 8.* Za dostup do MSP bi trebala biti upotrebljena lozinka i naziv korisnika odvojeno.

*Smjernica 9.* Lozinku bi trebalo mijenjati svakih 90 dana.

*Smjernica 10.* Tijekom procesa zamjene lozinke, kao novu se ne bi trebale upotrebljavati stare lozinke.

*Smjernica 11.* Ukoliko korisnik prekorači dozvoljeni broj pokusa ulaza u sistem, isti bi se trebao automatski isključiti i o tome upozoriti o voditelja sustava.

*Smjernica 12.* Strojna oprema kojom se obrađuju povjerljivi zdravstveni podaci bi trebao biti opremljen dodacima koji povećavaju pouzdanost i sigurnost sustava kao npr. sustavom za neprekidno napajanje (UPS), sustavom za zapis svih naredbi koje je kompjutor primio u zadnjih nekoliko trenutaka (engl. audit trail), zaštitom protiv instalacije sustava drugog diska itd.

*Smjernica 13.* Informatičko osoblje, koje brine za medicinski skup podataka ne bi smjelo imati ovlaštenja za uvid u isti, ukoliko sadrži osobne podatke.

*Smjernica 14.* Dokumenti i podaci na njima bi trebali biti označeni s obzirom na stupanj povjerljivosti (npr. bez oznake u slučaju opće dostupnosti, oznake "samo za internu upotrebu" u slučaju dostupnosti za sve zdravstvene djelatnike određenog

zavoda do oznake “povjerljiv document” u slučaju dostupnosti samo za ovlaštene korisnike)

*Smjernica 15.* Za demonstraciju, uvođenje novih ili provjeru starih aplikativnih programa bi se trebali upotrebljavati izmišljeni osobni podaci.

*Smjernica 16.* Broj osoba koje imaju pravo pristupa do osobnih podataka bi trebao biti ograničen na najmanju moguću mjeru. Na primarnom nivou bi to morao biti osobni liječnik ili liječnik koji ga zamjenjuje, na sekundarnom i tercijarnom nivou ekipa specijalista koji su neposredno uključeni u proces liječenja.

*Smjernica 17.* U svakom zdravstvenoj ustanovi bi trebala postojati evidencija unosa ili iznosa predmeta, dokumenata itd iz prostora u kojima se obrađuju ili čuvaju osobni podaci.

*Smjernica 18.* Analiza rizika je preporučljiva metoda vrednovanja mjera zaštite osobnih podataka koje upotrebljava vodstvo zdravstvene ustanove.

## **5. Načelo zabrane sakupljanja određenih osobnih podataka**

*Smjernica 1.* Osobni podaci koje se odnose na etničko ili rasno podrijetlo, političko uvjerenje, vjersko ili filozofsko uvjerenje, članstvo u političnim organizacijama i podaci koji se odnose na spolni život se ne bi smjeli sakupljati ukoliko ne postoji pojedinčeva suglasnost o njihovom sakupljanju. Iznimke se mogu odrediti samo zakonom.

## **6. Načelo medicinskih i epidemioloških istraživanja**

Odnos prema informacijskoj povjerljivosti je pretpostavljen interesima istraživanja. Pojedinaac mora biti točno u pismenom obliku upoznat s vrstom osobnih podataka koji će se upotrebljavati tijekom istraživanja, namjenom istraživačkog rada i tijekom istraživanja.

*Smjernica 1.* Osobni podaci koji se obrađuju trebali bi biti u obliku koji onemogućuje identifikaciju pojedinca

*Smjernica 2.* U slučaju da anonimnost implicira neizvedivost istraživanja (npr. praćenje), isto bi se trebalo nastaviti uz upotrebu osobnih podataka pod sljedećim uvjetima:

- da pojedinac da pismenu suglasnost ili
- uporabu osobnih podataka odobri moralno etička komisija

## ***Načela i smjernice zaštite osobnih podataka koja vrijede u privatnom sektoru***

### **1. Načelo zakonitosti**

Sakupljanje, obrada i posredovanje osobnih podataka u privatnom sektoru je zakonito samo ukoliko je pojedinac za to dao pismenu suglasnost.

### **3. PRIJEDLOG TEMPORA UVOĐENJA POJEDINIH MJERA**

U sustavu zdravstvene zaštite se sakuplja, kruži i razmjenjuje velika količina osobnih podataka. Neusklađenost između pravno formalnim i operativnim vidikom osiguravanja zaštite osobnih podataka zahtijeva cjelovit i sistematičan pristup rješavanju tog problema. Temeljne mjere zaštite osobnih podataka moraju biti definirane na nacionalnom nivou. Možemo ih definirati kao *kratkoročne i dugoročne* (19).

*Kratkoročne* mjere impliciraju trenutnu neusklađenost među pravno formalnim i konkretnim (operativnim) vidicima zaštite osobnih podataka i sadašnju neusklađenost aktivnosti na nacionalnom nivou. *Kratkoročne* mjere obuhvaćaju:

1. uređenje zakonske osnove za sakupljanje osobnih podataka u sustavu zdravstva.
2. određivanje nositelja tih aktivnosti na nacionalnom nivou a koji bi se tim područjem profesionalno bavio. Odgovoran bi bio za operativno pripravljanje programa i projekata te za koordinaciju rada projektnih grupa.
3. oblikovanje prijedloga pravilnika o zaštiti osobnih podataka u zdravstvenim ustanovama, koji bi pomagao izvođačima zdravstvene zaštite urediti to područje.
4. Uključivanje nositelja tih aktivnosti u aktivnosti koje teku u okviru projekta AIM Europske Zajednice ( prije SEISMED, sada ISHAR projekt, itd)

*Dugoročne* mjere impliciraju realizaciju određenih programa Komisije Europske Zajednice. Program bi se morao realizirati u sljedećim fazama:

1. faza – u obliku formalnog dokumenta
2. faza – u obliku operativnih uputa
3. faza – u obliku implementacije operativnih uputa u praksi
4. faza – u obliku evaluiranja i održavanja tih dokumenata

## 4. DALJNI SMJER RAZVOJA

Razvoj na području zaštite osobnih podataka se odvija u dva glavna smjera. Prvi je, da za sakupljanje, obradu i komunikaciju osobnim podacima mora postojati zakonska osnova (25). Najprecizniji dokument na tom području je svakako najnovija Direktiva Europske unije, koja definira više pravnih osnova za obradu osobnih podataka. Pored obvezne zakonske osnove u javnom sektoru ona za obradu osobnih podataka unutar privatnog sektora zahtijeva pismenu suglasnost pojedinca.

Na području komunikacije osobnim podacima razvoj ide u smjeru uvođenja asimetričnih kriptografskih metoda zaštite osobnih podataka. Kriptografija je znanost (matematička disciplina) o sakrivanju poruka. Većina europskih država koje imaju već drugu ili čak treću generaciju zakona o osobnim podacima u svoje je nacionalne zakone uključila odredbu o obveznoj uporabi kriptografske metode unutar sustava zdravstva tijekom komunikacije tim podacima. Kriptografija nudi takve algoritme i postupke koje određene datoteke učine nedostupnim neovlaštenim osobama. Metoda je sastavljena iz matematičke transformacije otvorenoga teksta u zatvoren – kriptiran tekst. Princip algoritama za taj postupak je opće poznat. Parametar za transformaciju se naziva ključ i u njemu leži cjelokupna sigurnost. Glavni problem sa kojim se susreću pojedine države tijekom uvođenja kriptografije kao metode je upravljanje ključevima, odnosno njihovo certificiranje. Danas su u uporabi dvije vrste kriptografskih algoritama. Prvi je simetrično kriptografiranje pri kojem su ključevi za zatvaranje i otvaranje datoteka isti. Na tom području su dobro znani DES (data encryption standard). To su brzi algoritmi u kojima se našem korespondentu mora dostaviti tajni ključ po posebno tajnom i sigurnom putu.

Druga vrsta kriptografskog algoritama je asimetrično kriptografiranje, na tom području je najpoznatiji RSA (Rivest, Shamir, Adleman) standard. Ta metoda upotrebljava dva ključa: javni i tajni ključ. Kada javnim ključem zatvorimo datoteku, nitko je ne može više čitati osim korespondenta koji ima tajni ključ.

Usko povezano uz područje kriptografskog algoritma je područje digitalnog potpisa u elektroničkoj izmjeni podataka koji u biti predstavlja nadomjestak vlastitog potpisa. Potpisivanje teče u dva koraka. Prvo transformiramo poruku odnosno podatke sa određenom funkcijom. Dobiveni blok nato šifriramo. Rezultat zovemo digitalni potpis. Digitalni potpis osigurava visok stupanj sigurnosti jer je u biti nemoguće naći dvije poruke istovjetnog sadržaja i da ujedno odgovaraju istoj funkciji (26, 27).

Među prioritarnim ciljevima Vijeća Europske Unije je područje zaštite privatnosti pojedinca. Kao zadnji primjer definiranja ciljeva mogu navesti konferenciju TIDE kluba 2000 (28). Posebno poglavlje je namijenjeno pravu u informacijskom dobu. U

njemu je kao izhodište postavljeno deset točki o prilikama i utjecaju uvođenja suvremenih modernih tehnologija na pojedinca i njegovu privatnost. To su:

1. Tehnološki razvoj ugrožava ljudska prava i zato zahtjeva odgovarajući odgovor.
2. Postojeće zakonodavstvo je u pojedinim državama na području zaštite privatnosti preskromno.
3. U nekim slučajevima sama tehnologija zahtijeva ili čak uzrokuje reforme pravnog sustava.
4. Pojedinac nije najbolji ocjenjivač vlastitih interesa. Zbog toga su potrebna posebna tijela, čija je dužnost identifikacija potencijalnih opasnih situacija koje mogu predstavljati kršenje prava.
5. Trošak zaštite privatnosti mora biti tijekom uspostave evidencije unaprijed uračunat
6. Informacijsko pravo se mora razvijati fleksibilno zbog brzog razvoja tehnologije i promjene problematike.
7. Zaštita privatnosti mora obuhvaćati javni i privatni sektor.
8. Informacijska tehnologija predstavlja međunarodna rješenja, što zahtijeva i međunarodno uređenje.
9. Pravni odgovori na probleme moraju biti usmjereni na realne probleme i ne smiju se baviti mitovima ili simbolima.
10. Demokratske vrijednosti moraju biti očuvane, zato je važno pitanje, da li sa postojećim institucijama može odgovarajuće odgovoriti na tehnološke izazove.

Na konferenciji je po prvi put uporabljen izraz "informacijsko pravo". Radi se o pojmu koji obuhvaća ona prava pojedinca koja su sa razvojem informacijskih tehnologija i njihovim uvođenjem u našu svakidašnjost postala ugrožena.

## 5. LITERATURA

1. Čebulj J. Varstvo informacijske zasebnosti v Evropi in v Sloveniji. Ljubljana: Inštitut za javno upravo, 1992:9-25.
2. Human Rights and Scientific and Technological Developments – Uses of effect the rights of the person and the limits which should be placed on such uses in a democratic society. UN, 1976
3. Convention No. 108 for the protection of individuals with automatic processing of personal Data, Comity of the Council of Europe, Strasbourg, 1981
4. Reglementation applicable aux banques de donnes medicales automatisees, Recommendation No. R(81)1 adopte par le Comite des Ministres du Conseil de l'Europe, Strasbourg 1981
5. Recommendation No. R(83) Comity of the Council of Europe, Strasbourg, 1983
6. Recommendation on the Protection of Medical Data R(96) of the Council of Europe, Strasbourg 1996 – Draft
7. European Union Directive 95/46/EC. On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. OJ L281/31, October 1995
8. Cannataci JA, Bonnici J. Medical data protection in Europe: New rules vs. actual trends. In: Strategic Alliances between Patient Documentation and Medical Informatics. Amsterdam: AMICE Conference, 1995: 301-321.
9. Barber B. Some Systems Implications of EU data Protection Directive. Proceeding of Medical Informatics Europe. IOS Press, 1997: 829-833.
10. Dolenc A. Medicinska etika in deontologija. Ljubljana: Tangram, 1993:145-188.
11. Deklaracija iz Lisabona o pravima bolesnika (34. Skupština SZO, 1981)
12. Opća deklaracija ljudskih prava – OZN, Prosinca 1948
13. Furnell SM, Gaunt PN, Holben RF et al. Assessing staf attitudes towards information security in a European healthcare establishment. Med Inform 1996; 21:105-112.
14. Zakon o varstvu osebnih podatkov, Ur.l. RS 8/90 in 26/92
15. Premik M. Zaščita medicinskih podatkov. Zbornik V posvetovanja o medicinski informatiki, Bled 1992; 61: 659-21.
16. A High Level Security Policy Dokument, Commission of the European Communities, Advanced Informatics in Medicine (AIM) Program; SEISMED (A2033) Project, 1993

17. Barber B. Towards an Information technology Security Policy for NHS. pp 345-351 in HC91 Current Perspectives in Healthcare Computing, British Journal of Healthcare Computing, 1991.
18. Jones PJ. Data Users must observe all Principles of Data Protection Act. BMJ 1996;313: 560.
19. Razvojno raziskovalni projekt "Elementi enotnosti zdravstvenega informacijskega sistema v Republiki Sloveniji". Inštitut za varovanje zdravja. Ljubljana 1994
20. Pas L., Azeredo Z., Gonzalez JA. Et all. Determinants of preventive primary health care. In: Pas L (ed). Proceedings of the WONCA satellite Conference. The Hague, 1993:147-149.
21. Gilley J. Women in general practice. London: General medical services committee, 1994:7-21.
22. Zdravstveno statistični letopis. Zdrav Var;36:437-38.
23. European study on task profiles of general practitioners 1993-1994, Nivel, 1997
24. Gritzalis D. Medical data protection: a proposal for a deontology code. J Med Syst 1990;14: 375-386.
25. Lavrenčič DD. O varovanju podatkov v zdravstvu. Infor. Med Slov 1994; 1:51-52.
26. National Bureau of Standards: Data Encryption Standard. Federal information processing standards publications 46 edition, NHS Management Executive, EL(92)60 September 1992
27. Kaliski B. The MD2 Message Digest Algorithm. RFC 1319, RSA Laboratories, 1992
28. Telecommunication, Information and Interdependant Economies – TIDE 2000, Amsterdam, 1995