Tehnička zaštita podataka i provođenje mjera sigurnosti

GDPR

GDPR

- U godinu dana objavljeno je oko 100 novčanih kazni - uključujući ogromnu kaznu od 57 milijuna dolara Googleu (Francuska) - što pokazuje da GDPR ima zube, a Europska unija ih se ne boji koristiti.
- Poznati hotelski lanac Marriott mogao bi biti kažnjen (UK) s čak 99 milijuna funti kazne zbog propusta u zaštiti privatnosti svojih gostiju te British Airways s kaznom u visini od 183,4 milijuna funti zbog curenja privatnih podataka pola milijuna klijenata.

GDPR

- Austrija - kaznilo je poduzetnika zbog kršenja pravila o video nadzoru u visini od 4.800 eura
- Njemačka – sankcija kompaniji zbog napada hakera te neovlaštenog pristupa i otkrivanja osobnih podataka približno 330 tisuća korisnika, uključujući lozinke i e-mail adrese.
- Portugal - sankciju od 400 tisuća eura bolnici koja nije zaštitila kliničke podatke pacijenata čime su oni bili dostupni neovlaštenim osobama

GDPR

- Poljska –kažnjeno je društvo u visini od 220 tisuća eura koje prikuplja osobne podatke iz javno dostupnih registara, u svrhu pružanja usluga procjene boniteta poduzetnika. Prikupljene i obrađene informacije obuhvaćaju osobne podatke više od 7 milijuna obrtnika (poduzetnika), a obavijesti o obradi na e-mail dobilo je samo 900.000 ispitanika. Ostalih oko 6 milijuna ispitanika nije obaviješteno jer voditelj obrade nije imao podatke o njihovim e-mail adresama

Zašto je to važno?

Na ime političara kupovao mobitele

Sumnjiče ga za još 20 kaznenih djela krađe identiteta i računalne prijevare kojima je građane oštetio za najmanje **34.500** kuna.
http://www.vecernji.hr/crna-kronika/ponovno-uhicen-na-ime-politicara-kupovao-mobitele-pa-prodavao-preko-oglasnika-976035

Lopovi na njezino ime kupili mobitele, ona dobila račune

Torbicu s osobnim dokumentima i bankovnim karticama ukrali su joj dok je bila u svatovima, a potom su je šokirali računom. Iako je zatražila da se zabrane dolazni i odlazni pozivi sa zaključenih pretplata, u međuvremenu joj je stigao novi račun, sada na 1500 kuna. Tako joj se ukupan dug "popeo" na **2.221,93** kune.

http://www.vecernji.hr/crna-kronika/lopovi-na-njezino-ime-kupili-mobitele-ona-dobila-racune-903169

U zatvoru odležao nevin godinu i pol dana

U osječkom je zatvoru završio jer je netko krivotvorio njegovu putovnicu, a koju je nekoliko godina prije izgubio. Oslobođen je optužbi nakon što je USKOK u Makedoniju poslao otiske njegovih prstiju.

http://www.vecernji.hr/crna-kronika/albanac-tahir-tairi-30-u-zatvoru-odlezao-nevin-godinu-i-pol-dana-478961

Neovlašteno ušao u računalni program i povisio si plaću!

Bio je zaposlen kao stručni suradnik za poslove javne nabave http://bit.ly/2isW1xZ

Zašto je to važno?

Krađa preko 130 milijuna kartica (SAD)

kompjuterskom provalom u baze podataka velikih maloprodajnih mreža ukrao podatke o vlasnicima kreditnih i platnih kartica
http://www.bug.hr/vijesti/krada-130-milijuna-kartica/98201.aspx
http://www.bug.hr/vijesti/kriv-kradu-kartica/98603.aspx

Rus ostavio novčanik u restoranu pa mu ispeglali kartice

Rus je s društvom bio u restoranu "Borak", na Putu Zlatnog rata u Bolu. Poslije večere platio je račun i otišao, no bez novčanika koji mu je ostao na stolu. Tek nakon pola sata 28-godišnji Rus primijetio je da mu "nešto nedostaje" pa je pohitao u restoran "Borak". Kasno. Novčanika više nije bilo. Nepoznati lopov s njegovih je kreditnih kartica uspio **"ispeglati" oko 25 tisuća kuna**. I to jako brzo.

http://www.vecernji.hr/crna-kronika/rus-ostavio-novcanik-u-restoranu-pa-mu-ispeglali-kartice-442714

Anonimni hakeri objavili osobne podatke više od 37 milijuna nevjernih supružnika s internetskog portala Ashley Madison

Hakeri su objavili da posjeduju sve te podatke, a danas su na jednoj stranici kojoj se pristupa posebnim softverima ostavili 9,7 gigabajta težak file na kojima se mogu pronaći email adrese, lozinke i bankovne transakcije korisnika Ashley Madisona.
http://www.jutarnji.hr/hakeri-razotkrili-preljubnike--objavljeni-podaci-milijuna-korisnika-stranice-za-preljubnike--medu-njima-politicari--vladni-duznosnici--bankari--cak-i-djelatnici-iz-vatikana-/1401546/

Zašto je to važno?

Cyber-napad na američki Ured za pohranu osobnih podataka zaposlenih (SAD)

Podaci iz zdravstvenih kartona sada vrijede 10 puta više od onih o nečijoj kreditnoj kartici jer se uz pomoć zdravstvenih podataka mogu stvoriti lažne kartice i podizati medicinska oprema, lijekovi i pomagala, te organizirati prijevare osiguravajućih kuća
http://www.novilist.hr/Znanost-i-tehnologija/Tehnologija/Zdravstveni-podaci-unosniji-od-karticnih

Hakeri upali u državni sustav i oteli osobne podatke svih građana? (Srbija)

Petorica mladih srpskih hakera provalili su u državni sustav i pokrali, kako tvrde, JMBG-ove gotovo svih građana Srbije
http://www.jutarnji.hr/-drzimo-srbiju-u-saci--srpski-hakeri-tvrde--ukrali-smo-gotovo-sve-jmbg-ove-gradana/1253240/

Yahoo potvrdio: Hakeri su ukrali podatke 500 milijuna korisnika!

Ukradena su, između ostalog, imena i elektronička pošta, kao i nešifrirana sigurnosna pitanja i odgovori. Nisu ukradeni podaci o kreditnim karticama
https://www.vecernji.hr/techsci/yahoo-potvrdio-hakeri-su-ukrali-podatke-500-milijuna-korisnika-1115758

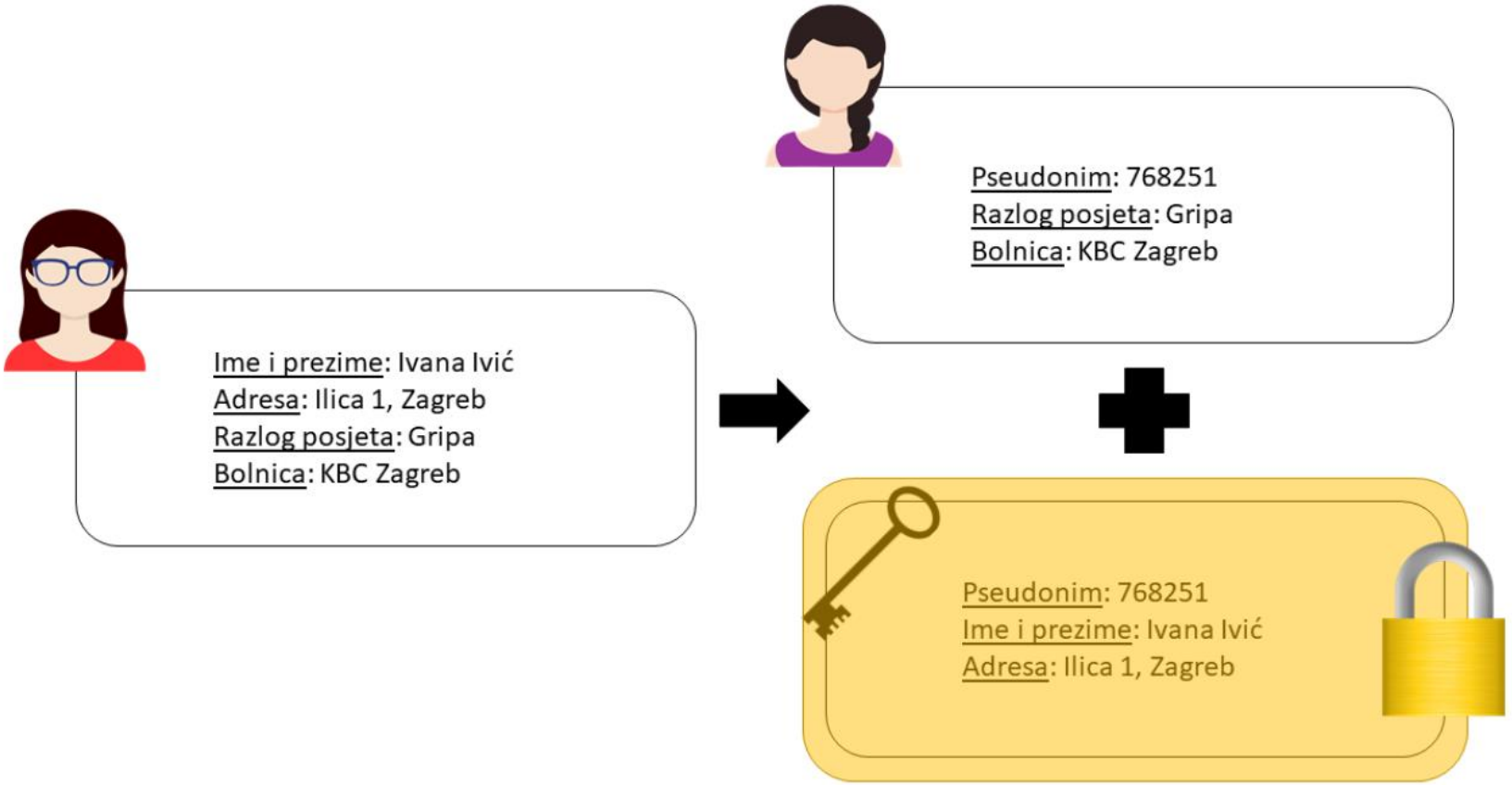
Kako se uskladiti sa GDPR-om?

1. Evidentirajte svoje podatke
2. Utvrdite tko je odgovoran za podatke koje koristite
3. Implementirajte odgovarajuće mjere za zaštitu podataka
4. Ustrojite postupke za djelovanje u slučaju sigurnosnih incidenata
5. Imenujte službenika za zaštitu osobnih podataka
6. Razvijte kulturu zaštite podataka na svim razinama organizacije
7. Provodite edukacije

Mehanizmi zaštite podataka

- **Pseudonimizacija podataka** (…osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija…). Osobnim podacima se umjesto pravog identifikatora (npr. OIB-a) dodjeljuje zamjenska vrijednost (pseudonim). Pseudonimizacija nije obavezna, ali je svakako odlična praksa u dizajnu informacijskih sustava. (https://www.cert.hr/wp-content/uploads/2018/08/anonimizacija_i_pseudonimizacija_podataka.pdf)

Primjer pseudonimizacije podataka na jednom zapisu



Izvor: CERT.hr

Primjer pseudonimizacije tokenizacijom

Ime i prezime	Adresa	Spol	Datum rođenja	Razlog posjeta	Bolnica
Ivana Ivić	Ilica 1	Ž	5.9.1980.	Gripa	KBC Zagreb
Jakov Marić	Žuta obala 3	M	30.1.1988.	Operacija oka	KBC Split
Ema Novak	Maksimir 76	Ž	23.4.2007.	Lom čeljusti	KBC Zagreb
Marko Jurić	Šegrtova 4	M	17.8.1987.	Ubod ose	KBC Pula
Lucija Perić	Ribarska 51	Ž	6.12.1995.	Trudovi	KBC Osijek
Luka Matić	Vinogradi 25	M	12.5.1972.	Povraćanje	KBC Zadar
Ana Babić	Splitska 89	Ž	9.4.1969.	Srčani udar	OB Koprivnica

Token	Spol	Datum rođenja	Razlog posjeta	Bolnica
621971	Ž	5.9.1980.	Gripa	KBC Zagreb
781365	M	30.1.1988.	Operacija oka	KBC Split
436851	Ž	23.4.2007.	Lom čeljusti	KBC Zagreb
562799	M	17.8.1987.	Ubod ose	KBC Pula
162484	Ž	6.12.1995.	Trudovi	KBC Osijek
957316	M	12.5.1972.	Povraćanje	KBC Zadar
242351	Ž	9.4.1969.	Srčani udar	OB Koprivnica

Token	Ime i prezime	Adresa
621971	Ivana Ivić	Ilica 1
781365	Jakov Marić	Žuta obala 3
436851	Ema Novak	Maksimir 76
562799	Marko Jurić	Šegrtova 4
162484	Lucija Perić	Ribarska 51
957316	Luka Matić	Vinogradi 25
242351	Ana Babić	Splitska 89

Izvor: CERT.hr

Primjer pseudonimizacije šifriranjem

Ime i prezime	Adresa	Spol	Datum rođenja	Razlog posjeta	Bolnica
Ivana Ivić	Ilica 1	Ž	5.9.1980.	Gripa	KBC Zagreb
Jakov Marić	Žuta obala 3	M	30.1.1988.	Operacija oka	KBC Split
Ema Novak	Maksimir 76	Ž	23.4.2007.	Lom čeljusti	KBC Zagreb
Marko Jurić	Šegrtova 4	M	17.8.1987.	Ubod ose	KBC Pula
Lucija Perić	Ribarska 51	Ž	6.12.1995.	Trudovi	KBC Osijek
Luka Matić	Vinogradi 25	M	12.5.1972.	Povraćanje	KBC Zadar
Ana Babić	Splitska 89	Ž	9.4.1969.	Srčani udar	OB Koprivnica

Šifrirano ime, prezime i adresa	Spol	Datum rođenja	Razlog posjeta	Bolnica
LWrGYUkILOxferCNXZVc...	Ž	5.9.1980.	Gripa	KBC Zagreb
GrRuyibVKrIjfNapLyIH...	M	30.1.1988.	Operacija oka	KBC Split
IZjHkZNZCRSqnTXKdTEr...	Ž	23.4.2007.	Lom čeljusti	KBC Zagreb
KDzPTWaCPAreYKtrGwdf...	M	17.8.1987.	Ubod ose	KBC Pula
rurAMuRDHwtFiORyIEUL...	Ž	6.12.1995.	Trudovi	KBC Osijek
NKSuGSKZLWuzgiWHtZqu...	M	12.5.1972.	Povraćanje	KBC Zadar
CrLGxYmCQKpsdUFVbHDv...	Ž	9.4.1969.	Srčani udar	OB Koprivnica

Tajni ključ za šifriranje

Izvor: CERT.hr

Primjeri

- I dalje nije u potpunosti jasno postižu li današnje tehnike anonimizacije i pseudonimizacije očekivani rezultat te kako će se one nositi s budućim otkrićima. No u konačnici, neosporno je da one otežavaju reidentifikaciju i time smanjuju potencijalnu štetu prilikom povrede osobnih podataka, te je zato i njihova korist **prepoznata u regulativi**.

Izvor: CERT.hr

Mehanizmi zaštite podataka

- **Enkripcija** je postupak šifriranja podataka na način koji sprječava neovlaštene osobe da ih pročitaju.
- Savjet oko šifriranja odnosi se uglavnom na zahtjev da se on postavi na odgovarajući način na razinu rizika ili osjetljivosti podataka. Naglasak je na uspostavi politike šifriranja i na obučavanju osoblja. Treba uzeti u obzir smjernice vezane za sektor. Treba koristiti šifrirane komunikacijske kanale. Pri implementaciji šifriranja valja uzeti u obzir četiri stvari: **odabir pravog algoritma, prave veličine ključa, pravog softvera i čuvanje ključa**. Rješenja treba redovito pregledavati kako bi se osigurala adekvatna zaštita i sukladnost s trenutnim standardima.

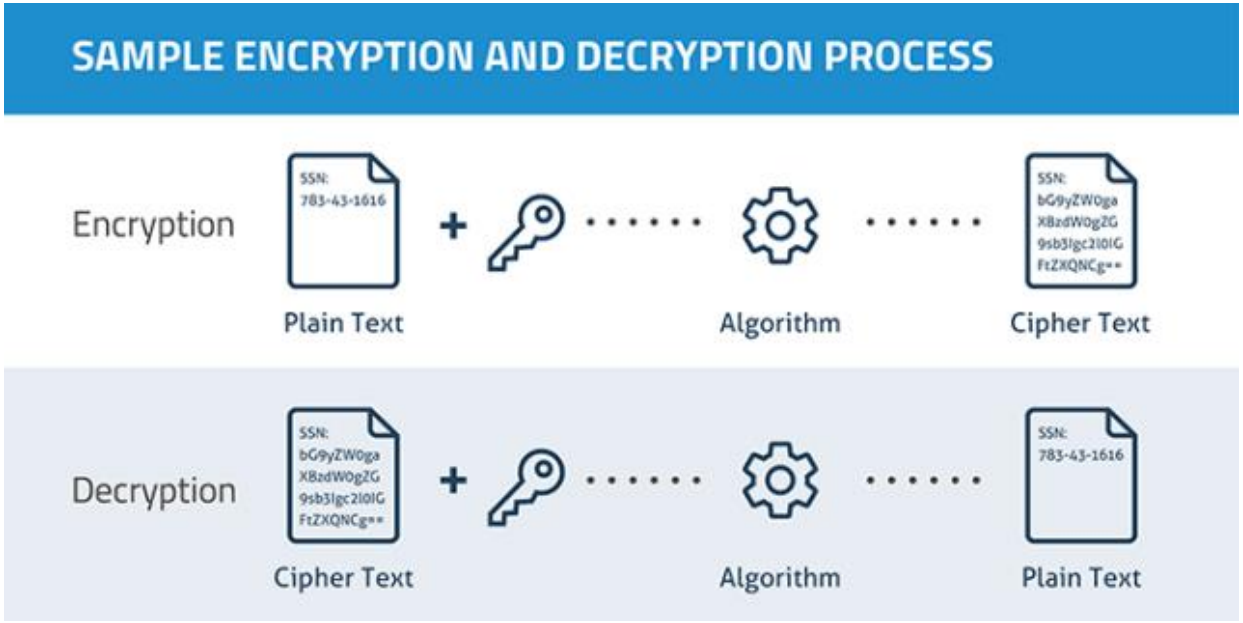
Mehanizmi zaštite podataka

- Enkripcija se obično primjenjuje na dva načina:

  Enkripcija spremišta – *često nazivanog "podaci u mirovanju"* –predstavlja najčešći način enkripcije čitavog diska, pogona ili uređaja. Ova vrsta enkripcije stupa u funkciju tek nakon prestanka rada sustava, isključivanja pogona ili blokiranja ključa za enkripciju.

  Enkripcija sadržaja – *poznata kao "granularna enkripcija"* – tipično označava enkripciju datoteka ili teksta na razini aplikacije. Najbliži primjer je enkripcija e-mail poruka, gdje format poruke mora ostati netaknut kako bi ga klijent mogao obraditi, ali se tijelo e-mail poruke zajedno sa svim prilozima šifrira.

Kako to radi?



Besplatni alati:

Enkripcija e-mail poruka i datoteka:
https://www.gpg4win.org/

Enkripcija diskova i datoteka:
https://www.veracrypt.fr/en/Home.html

Mehanizmi zaštite podataka

- **Lozinke** se trebaju upotrebljavati samo tamo gdje je to prikladno - potrebna je viša razina sigurnosti. Dobar sustav lozinki trebao bi napadačima otežati pristup pohranjenim lozinkama u upotrebljivom obliku i trebao bi zaštititi od napadača. No, pojedince se ne bi smjeli prekomjerno opterećivati bilo da se sjećaju lozinke ili da bi bili sigurni da je račun siguran. Treba koristiti odgovarajući algoritam raspršivanja ili drugi mehanizam koji nudi sličnu zaštitu. Arhitektura sustava mora spriječiti curenje lozinki. Stranice za prijavu trebaju biti zaštićene https, a hashing se treba provoditi na poslužitelju, a ne na strani klijenta.

Mehanizmi zaštite podataka

- Treba postaviti odgovarajuću duljinu lozinke, ali ne i maksimalnu, osim ako to nije apsolutno neophodno. Popis zaporki je dobar način da se spriječi uporaba predvidljivih lozinki. Ne bi trebalo postojati druga ograničenja u vezi s stvaranjem lozinke. Broj pogrešnih pokušaja prijave mora biti ograničen ili ugašen, ali ne smije biti nizak. Mogle bi se upotrijebiti i druge metode sprečavanja napada poput upotrebe CAPTCHA, vremenskih ograničenja ili kašnjenja nakon neuspjele prijave. Treba koristiti pristup temeljen na riziku provjere autentičnosti. U nekim slučajevima može biti prikladno zatražiti drugu provjeru autentičnosti koja može biti na primjer biometrijskim ili jednokratnim znakom.

Mehanizmi zaštite podataka

- Velika većina nas je kriva za korištenje istih ili sličnih lozinki u nizu aplikacija i web stranica ili za korištenje očiglednih lozinki. U eri u kojoj malo vjerovatno ne znamo više od jednog ili dva telefonska broja, sjećanje na mnoštvo lozinki neće doći lako većini nas. Zanimljivo je i da su korisnici protiv trenutnog trenda obavezne uključivanja posebnih znakova ili barem jednog broja.
- Poduzeća moraju sama odrediti koje će vrste šifriranja i lozinke koristiti, ali što se tiče zaposlenika ili kupaca, nije rijedak slučaj da će najprikladnije biti i tehnički najsloženije rješenje.

Mehanizmi zaštite podataka

Back-up i pravo na zaborav

- Postoje dva pitanja koja imaju mogućnost građanina EU-a da zatraži od organizacije uklanjanje svih podataka. Prvo je pitanje "Sadrži li zahtjev za brisanje uklanjanje podataka iz sigurnosnih kopija?„
- Organizacije moraju jasno objasniti subjektu podataka da su njegovi osobni podaci uklonjeni iz aktivnih sustava, u sigurnosnoj kopiji su ostali, ali će biti uklonjeni nakon određenog vremena (naznačite vrijeme zadržavanja u svojoj komunikaciji sa subjektom podataka).

Mehanizmi zaštite podataka

- Drugo pitanje je da će organizacija, ukoliko izbriše zapis, a zatim ga vrati iz starije sigurnosne kopije (koja sadrži sada izbrisani zapis), izbrisani zapis vratiti u uprabu, što je neprihvatljivo
- Savjetuje se da organizacije moraju održavati indeks traženih brisača - koristeći neoznačive markere, poput broja redaka baze podataka, a ne osobnih detalja - koji odgovaraju zadanom vremenu zadržavanja sigurnosne kopije. Na ovaj način, ako se za oporavak zahtijeva starija sigurnosna kopija koja sadrži sada izbrisane zapise, može se dogoditi ponovno brisanje takvih zapisa.

Tehničke i organizacijske mjere

- „U većini slučajeva curenja podataka koje je analizirao NSA tim uzrok je bio phishing e-mail ili nepatchirani sustavi” - David Hogue, a senior technical director for the NSA’s Cybersecurity Threat Operations Center
- Phishing – upoznati zaposlenike sa tipičnim phising mailovima (koliko zaposlenika je prijavilo sumnjiv e-mail?)
- Nepatchirani sustavi - iskorištavanje poznatih ranjivost predstavlja daleko realniji scenarij (SANS → preko 80% sigurnosnih incidenata odnosi se na iskorištavanje poznatih ranjivosti)

Uništavanje podataka

- Čuvanje podataka minimalno koliko je potrebno
- „Zbog toga je osobito potrebno osigurati da je razdoblje u kojem se osobni podaci pohranjuju ograničeno na strogi minimum”
- Brišete li podatke svojih korisnika? Ili ih čuvate zlu ne trebalo?

Upravljanje incidentima

- Očekuje se primjerena reakcija u slučaju incidenta
- „ …čim voditelj obrade primijeti da je došlo do povrede osobnih podataka, trebao bi o tome izvijestiti nadležno nadzorno tijelo bez nepotrebnog odgađanja i to, ako je izvedivo, najkasnije 72 sata…”
- Upadi u sustave mogu biti neprimijećeni danima
- Veće vrijeme otkrivanja incidenta znači i veću štetu (Yahoo primjer)

Upravljanje incidentima

- Mnogi smatraju da su sigurnosni incidenti neizbježni
- Potrebna promjena pristupa inf. sigurnosti
- „Nama se to ne može dogoditi” → „Dogodit će nam se ali ćemo to brzo otkriti”

Trošak neusklađenosti

AZOP prati usklađenost, a rad je usklađen na razini EU-a. Trošak nepridržavanja pravila može biti visok.

Hvala na pažnji!

GDPR brošura
https://www.konto.hr/informativna-brosura-o-gdpr/