Schrems II

Uppdaterad information

2020-12-03

Patrik Jonasson

Dataskyddsförordningen på 1 minut

- *Till skydd för mänskliga rättigheter*
- *Underlätta digitalisering*
- *Sanktionsavgifter och skadestånd-även för myndigheter*
- *Ger massor mer goda effekter*
- *Allt är inte klart än, exempelvis Schrems II*

- FN 1948
- Europarådet 1950
- Svensk lag 1994:1219

- ARTIKEL 8:
  Rätt till skydd för privat- och familjeliv
  1. Var och en har rätt till skydd för sitt privat och familjeliv, sitt hem och sin korrespondens.
  2. Offentlig myndighet får inte ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

Del 1. Schrems II-vad innebär detta egentligen?

Edward Snowden

Max Schrems

Ordlista-Personuppgifter

varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet

Dvs allt som direkt eller indirekt kan kopplas till en levande människa

Ordlista-EDPB

European Data protection Board (Dataskyddsstyrelsen)

Ordlista-Tredje land

Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området.

Obs! Att publicera något på internet är inte tredjelandsöverföring om webbplatsen lagras hos en internetleverantör som är etablerad inom EU/EES.

Exempel på överföring av personuppgifter till tredje land:

När ni skickar dokument som innehåller personuppgifter per e-post till någon i ett land utanför EU/EES.

När ni anlitar ett personuppgiftbiträde i ett land utanför EU/EES.

När ni ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.

När ni lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES.

När ni lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES.

När lagar i ett land gör att personuppgifter förs över till det landet, även om tjänsten driftas inom EU/ESS

Ordlista-Adekvat skyddsnivå

EU-kommissionen kan fatta beslut om att ett land har en tillräckligt hög skyddsnivå och ni får då föra över personuppgifter dit utan något särskilt tillstånd. I dataskyddsförordningen kallas det för adekvat skyddsnivå. Det kan även gälla ett visst territorium, en internationell organisation eller en eller flera sektorer i ett tredje land.

När EU-kommissionen fattar beslut om adekvat skyddsnivå tittar de bland annat på landets lagar och internationella åtaganden, vilka möjligheter den registrerade har att få rättslig prövning och om landet respekterar de mänskliga rättigheterna och de grundläggande friheterna. EU-kommissionen kontrollerar också att det finns oberoende tillsynsmyndigheter som ansvarar för att dataskyddsreglerna följs och som kan hjälpa de registrerade.

Obs! Till skillnad från i personuppgiftslagen finns det inte längre utrymme för den personuppgiftsansvarige att själv avgöra om det finns en adekvat skyddsnivå eller inte. Det är bara EU-kommissionen som kan fatta ett sådant beslut.

Ordlista-Länder med adekvat skyddsnivå

Länder med adekvat skyddsnivå

EU-kommissionen har fattat beslut om att skyddsnivån i dessa länder är adekvat, det vill säga tillräckligt hög enligt dataskyddsförordningen:

Andorra
Argentina
Bailiwick of Guernsey
Färöarna
Isle of Man
Israel
Japan
Jersey
Nya Zeeland
Schweiz
Uruguay

Dessutom har EU-kommissionen bedömt att skyddsnivån är adekvat på vissa områden eller under särskilda villkor i följande länder:

Kanada, om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling.

USA har alltså inte adekvat skyddsnivå

USA har alltså inte adekvat skyddsnivå

Vad gör USA?

Prism är ett signalspaningsprogram som används av amerikansk underrättelseverksamhet för insamling av uppgifter från hela världen. Dokument som den tidigare CIA-anställde visselblåsaren Edward Snowden läckte i juni 2013 visar att programmet har gett NSA och FBI tillgång till realtidskommunikation såväl som lagrad information från människor över hela världen via nio Internet-företag: Microsoft anslöts 2007 (inklusive Skype 2011), Yahoo! 2008, Facebook 2009, Paltalk 2009, Google 2009 (inklusive Youtube 2010), AOL 2011 och Apple 2012. Data som amerikanska myndigheter kan inhämta med Prism inkluderar inloggningsuppgifter, e-post, meddelanden på sociala nätverk, porträttfotografier (som kan användas för ansiktsigenkänning), videoklipp, video- och röstchatt, IP-telefoni och filöverföringar. I de läckta dokumenten anges att Prism:s signalspaning är "den främsta källan för underrättelser i NSA:s analysrapporter", och ofta används i analysrapporter till presidenten.
Avslöjandet visar att även personer i USA avlyssnats i stor skala, men enligt chefen för National Intelligence James Clapper får Prism inte avsiktligen användas för insamling riktad mot amerikaner eller någon i USA. Insamling av utländska underrättelser är emellertid tillåtet enligt avsnitt 702 av Foreign Intelligence Surveillance Act (FISA) från 1978 med tillägg från 2008. Enligt Clapper övervakas programmet av en särskild domstol, kongressen samt den verkställande makten, och säkerställer enligt honom att insamling, lagring och spridning av uppgifter om amerikaner av misstag ska hållas till ett minimum.
PRISM är en efterföljare till det Terrorist Surveillance Program som startades efter 11 september-attackerna. Enligt NSA:s whistleblower William Binney fyller PRISM hål i de underrättelser som NSA sedan länge insamlar via nätleverantörer, och ger FBI bevisning i domstolar.

USA har inte adekvat skyddsnivå

Problemet är lagarna Cloud Act och Fisa 702

USA har inte adekvat skyddsnivå

Regelverket i USA

- **CLOUD act,** 2018

> …an electronic communication service (ECS) or remote computing service (RCS) provider must comply with existing requirements to preserve, backup, or disclose the contents of an electronic communication or noncontent records or information pertaining to a customer or subscriber, regardless of whether the communication or record is located within or outside the United States.
>
> *Summary* H.R. 4943, *115th Congress 2017-2018*

USA har inte adekvat skyddsnivå

Regelverket i USA

- **Foreign Intelligence Surveillance Act,** 1978 (*FISA*)
- **FISA section 702,** 2008

> [Section 702] …permits the government to conduct targeted surveillance of foreign persons located outside the United States, with the compelled assistance of electronic communication service providers, to acquire foreign intelligence information.
> Office *of the* Director *of* National Intelligence (*ODNI)*

USA har inte adekvat skyddsnivå

Lösning: år 2000 Safe Harbour

Safe Harbor är en samling frivilliga regler om personlig integritet och dataskydd som tagits fram av USA:s handelsdepartement. Organisationer i USA har kunnat anmäla att de frivilligt ansluter sig till dessa regler. Baserat på detta undantag har europeiska organisationer genom globala avtal och system kunnat överföra personuppgifter till Safe Harbor-registrerade organisationer.

Max Schrems och Schrems I

Max Schrems, en ung österrikisk jurist och aktivist, bad Facebook år 2011 att delge honom all information de hade om honom. Han fick då en cd-skiva från Facebook som omfattade 1200 sidor av information om hans liv. I cd-skivan kunde man bland annat läsa om de privata meddelanden han skickat, evenemang han deltagit i och saker han gillade. Schrems bad därför 2013 den irländska dataskyddskommissionen att stoppa Facebook från att överföra hans privata information till USA, en klagan som gick ända till EU-domstolen.

Privacy Shield

Lösning: 2016 Privacy shield

Privacy Shield är en mekanism för självcertifiering som finns i USA. Det innebär att företag i USA kan anmäla sig till det amerikanska handelsdepartementet (Department of Commerce) och meddela att de uppfyller de krav som ställs i Privacy Shield. Enligt ett beslut från EU-kommissionen har det varit tillåtet för personuppgiftsansvariga i EU att överföra personuppgifter till mottagare som har anslutit sig till Privacy Shield. Sedan juli 2020 är dock Privacy Shield ogiltigförklarat och kan inte längre användas.

Skillnader:

Are there a lot of differences between the agreements? Not really. The differences between Safe Harbor and Privacy Shield are more in the methods of addressing data transfers than changing the nature of them. Safe Harbor had seven principles: Notice, Choice, Onward Transfers (transfers to third parties), Access, Security, Data Integrity, and Enforcement. Privacy Shield has those same principles, but focuses on more individual rights for EU citizens, stricter requirements for U.S. businesses and restricting U.S. government access to personal data.

One major change from Safe Harbor is the transfer of data to third parties, or the Onward Transfers principle. In the old agreement, an organization had to provide notice and choice to consumers before sharing personal information with a third party, but that was **not** required if the third party was "acting as an agent to perform tasks on behalf of and under the instructions of third organization."

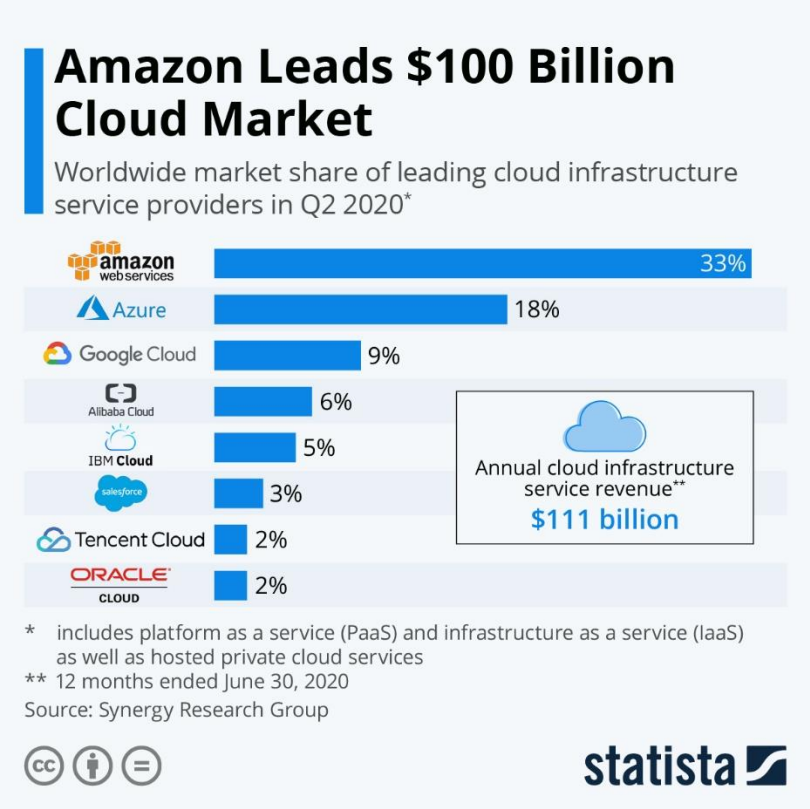
With the new agreement, that rule has changed dramatically. Companies who wish to transfer data to third parties now must also comply with the principle of purpose limitation and ensure that the third party provides **the same level of Privacy Shield protection as the original company.** Organizations must also provide a copy of relevant portions of its privacy agreement with the third party to the Department of Commerce upon request. However, even when those requirements have been met, an organization **remains liable** if the third party does not process the information in a manner consistent with Privacy Shield, unless it **proves it is not responsible** for any event that causes damage to the p

Schrems II

Privacy Shield ogiltigförklaras då amerikanska regelverk (såsom som FISA 702 och Cloud Act) möjliggör för amerikanska myndigheter att få tillgång till personuppgifter som överförs från EU till USA för nationella säkerhetsändamål, vilket leder till begränsningar av skyddet för personuppgifter såsom det reglerats i EU:s dataskyddslagstiftning.

EU-domstolen anför också att den amerikanska lagstiftningen inte innehåller några rättigheter för registrerade som kan göras gällande inför domstol mot de amerikanska myndigheterna.

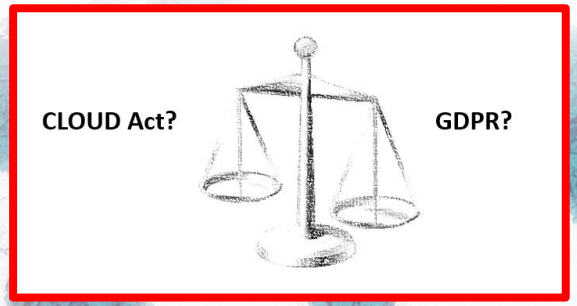
Utmaning: Trender inom IT



https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Problemet: EU:s stadgar vs USA:s lagar

Regelverk?



Datainspektions rekommendationer- innan EDPB:s förtydligande

Det första ni bör göra är att kartlägga vilka flöden av personuppgifter som finns i organisationen och i vilka fall personuppgifter kan komma att överföras till tredje land. Om uppgifter överförs till tredje land bör ni försöka utröna hur skyddet hos det mottagande landet ser ut i det särskilda fallet. Därefter måste ni ta ställning till om det finns stöd för överföringen eller inte.

I era avtal med eventuella personuppgiftsbiträden ska det framgå om personuppgifter överförs till tredje land. Ni bör även ta reda på om eventuella underleverantörer överför uppgifter till tredje land. Många tjänster överför idag uppgifter till tredje land.

Vad rekommenderade jag mina kunder innan EDPB:s förtydligande?

Identifiera tredjelandsöveröringar, primärt mot USA
Påbörja inga nya tjänster mot tredje land, primärt mot USA
Undersök vilka alternativ vi har som inte omfattar tredjelandsöverföringar
Jag omvärldsbevakar och ger fortlöpande rekommendationer till er

EDPB rekommendationer från den 10 november

- Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- Recommendations on the European Essential Guarantees for surveillance measures

Vad de säger

- Om SCC används måste PUA säkerställa att om inte landet har en adekvat skyddsnivå så måste PUA kompensera med lämpliga skyddsåtgärder, hur ska detta gå till?

https://www.linkedin.com/pulse/v%25C3%25A4gen-fram%25C3%25A5t-efter-edpbs-nya-rekommendationer-daniel-melin/?trackingId=4vNqNv7CQ9SUqAalPYk4Xw%3D%3D

Förtydligande från EDPB 10 november:

Use Case 1: Data storage for backup and other purposes that do not require access to data in the clear

79. A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes.

If

1. the personal data is processed using strong encryption before transmission,
2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
3. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,

4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
5. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and
6. the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,

then the EDPB considers that the encryption performed provides an effective supplementary measure.

Förtydligande från EDPB 10 november:

Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear

88. A data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country.

If

1. a controller transfers data to a cloud service provider or other processor,
2. the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,[71]

[71] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations on the European Essential Guarantees for Surveillance Measures.

then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.

Förtydligande från EDPB 10 november: Tolkning Daniel Melin, Skatteverket

- EDPB gör tydligt att det inte finns några ”harmlösa personuppgifter”.
- EDPB gör tydligt att bara det faktum att myndigheter i tredje land har samlat in personuppgifter är ett intrång i privatlivet. De behöver alltså inte göra något med dem.
- EDPB gör tydligt att tredje lands lagstiftning inte kan bedömas med en sannolikhetsprövning. Istället ska lagstiftning bedömas binärt.

https://www.linkedin.com/pulse/v%25C3%25A4gen-fram%25C3%25A5t-efter-edpbs-nya-rekommendationer-daniel-melin/?trackingId=4vNqNv7CQ9SUqAalPYk4Xw%3D%3D

NOYB: inlämnat 101 klagomål mot 3:e-landsöverföringar

- 17: augusti: 101 organisationer, varav sex svenska företag rapporterade till olika dataskyddsmyndigheter inom EU för att de använder Google Analytics eller Facebook connect
- 26:e november inledde Datainspektionen en granskning mot sex svenska företag som en del av ett EDPB-uppdrag
- De svenska är
- Qliro Group AB cdon.fi
- Sinovum Media AB synonymer.se
- Modern Women Media Sweden AB familjeliv.se
- Coop Sverige AB coop.se
- Dagens industri di.se
- Tele2 Sverige AB tele2.se

https://www.linkedin.com/pulse/v%25C3%25A4gen-fram%25C3%25A5t-efter-edpbs-nya-rekommendationer-daniel-melin/?trackingId=4vNqNv7CQ9SUqAalPYk4Xw%3D%3D

Max Schrems om Microsofts “defending your data” 19:e november

- First, we are committing that we will challenge every government request for public sector or enterprise customer data – from any government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.
- Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure.

We call these protections Defending Your Data, and we will begin adding them to our contracts with public sector and enterprise customers immediately.

Defending Your Data makes a substantial addition to our foundational privacy promises, and builds on the strong protections we already offer customers.

- **We use strong encryption:** We encrypt customer data with a high standard of encryption both when it is in transit and at rest. Encryption is a critical point in the draft EDPB recommendations. We do not provide any government with our encryption keys or any other way to break our encryption.
- **We stand up for customer rights:** We do not provide any government with direct, unfettered access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with demands when we are clearly compelled to do so. Our first step is always to attempt to re-direct such orders to customers or to inform them, and we routinely deny or challenge orders when we believe they are not legal.
- **We are transparent**: We have, for many years, published information about government demands for customer data. We sued the U.S. government over the ability to disclose more data about the national security orders we receive seeking customer data and reached a settlement enabling us to do so. As a result, twice a year, we disclose more detailed information about these national security orders across all our businesses (consumer, enterprise, and public sector), in addition to our regular Law Enforcement Request Report.
- **We have a track record of legal success.** We have more experience than any other company going to court to establish the limits of government surveillance orders, and we have even taken one case to the U.S. Supreme Court. Our efforts have provided customers with greater transparency and stronger protections. No commitment to challenge access orders can assure victory, but we feel good about our record of success to date.

Duty under Article 6(1)(c) – if there is no duty to comply (illegal request) then you can‘t provide the data… Challinging it is the logical consquence - nothing new…

Duty under Article 82 GDPR, but without all the limits (no class action, burden of proof on the user, etc) that Microsoft put into it‘s contract and that would actually limit (!) data subejcts‘ (third party) rights!

Required under Article 32 GDPR - big News.

Yeah, so Microsoft complies with FISA 702 which is the „legal process“.

Yeah, so you even disclose that you provided the data of 28.500 to 29.998 accounts in 2019.

Congrats, good job on SCA – but frankly overturend by the Cloud Act and irrelevant when this is about FISA 702.

https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/
https://twitter.com/maxschrems/status/1329802283341770752

Vad rekommenderar jag mina kunder idag

Identifiera tredjelandsöveröringar, primärt mot USA
Påbörja inga nya tjänster mot tredje land, primärt mot USA
Undersök vilka alternativ vi har som inte omfattar tredjelandsöverföringar
Gävle: Ovanstående presenteras till PUA och DSS under vecka 49
Ersätt Google Analytics med Matomo eller annan produkt/tjänst som ej omfattas av Schrems II
Jag omvärldsbevakar och ger fortlöpande rekommendationer till er

Vilka lösningar ser jag idag?

- USA förändrar FISA 702 och Cloud Act
- EU ändrar stadgan
- Egen drift
- Tjänsteleverantörerna anpassar sina affärsmodeller så de kan levereras av organisationer som inte omfattas av Schrems II
- Använd inga tjänster som omfattas av Schrems II (gäller även underleverantörer)

Frågor

Del 3. Nyheter hösten 2020

Datainspektionen byter namn 2021-01-01

Datainspektionen blir Integritetsskyddsmyndigheten, IMY

Den 1 januari 2021 byter Datainspektionen namn och blir Integritetsskyddsmyndigheten. Förkortningen blir IMY.

Lyssna

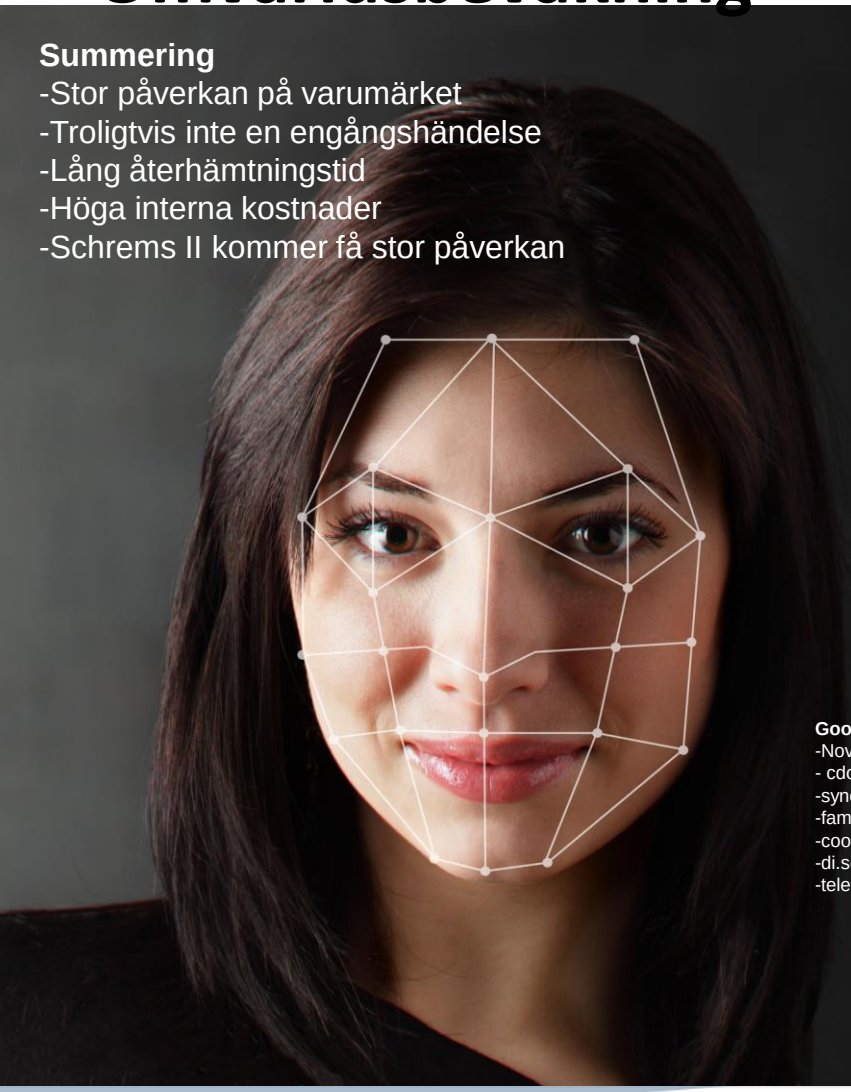
Vid årsskiftet byter Datainspektionen namn till Integritetsskyddsmyndigheten efter beslut från riksdagen. Förkortningen på myndigheten blir IMY. Namnbytet signalerar det förändringsarbete som redan pågår på myndigheten sedan införandet av dataskyddsförordningen, GDPR.

– Vi är en myndighet i förändring. Det utökade uppdrag vi fick i samband med dataskyddsreformen 2018 ställer krav på en utvecklad verksamhet för att kunna möta medborgarnas och verksamheternas behov. Namnbytet är välkommet och ger oss ny kraft att arbeta med vårt grundläggande uppdrag, att ta tillvara medborgarnas rättigheter i integritetsfrågor, säger Lena Lindgren Schelin, generaldirektör.

I grunden har IMY samma uppdrag som Datainspektionen. Det innebär fortsatt arbete för att skydda medborgarnas personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer.

Omvärldsbevakning

Summering
-Stor påverkan på varumärket
-Troligtvis inte en engångshändelse
-Lång återhämtningstid
-Höga interna kostnader
-Schrems II kommer få stor påverkan



Vastaamo

-Oktober 2020

-40 000 patientjournaler

-Inga sanktionsavgifter än

-VD sparkad

Skolplattform Stockholms stad
-November 2020
500 000 elever
Känsliga personuppgifter, skyddade identiteter
-4 miljoner SEK sanktionsavgift

Gunnebo
-Oktober 2020
-Känslig kundinformation

British Airways
- 2018. Beslut i oktober
-400 000 kunder
-kreditkortsuppgfter mm
-ca € 20 000 000 sanktionsavft

LSS-boende i Gnosjö
- November 2019
-Kamerabevakning sovrum
-200 000 sanktionsavgift

Google Analytics-Schrems II
-November 2020
- cdon.fi
-synonymer.se
-familjeliv.se
-coop.se
-di.se
-tele2.se

Tunstall
-Oktober 2020
-Patient dog
-Inga sanktionsavgifter än