JÖNKÖPING UNIVERSITY

Integritet på webb

GDPR och e-direktivet

2023-02-23

PRESENTATION

- Oskar Westergren (Dataskyddsombud)

DEL 1 – GDPR

DATASKYDDSFÖRORDNINGEN (GDPR)

EU:s stadga om de grundläggande rättigheterna:

- rätt till respekt för sitt privatliv och familjeliv (Art 7)
- skydd av personuppgifter (Art 8)

Avsikterna med GDPR är att:

- EU-medborgare ska få kontroll över sina personuppgifter,
- stärka skyddet för personuppgifter inom EU, och
- förenkla regelverk för internationella företag.
- beivra överträdelser mot rätten till privatliv och skydd av personuppgifter

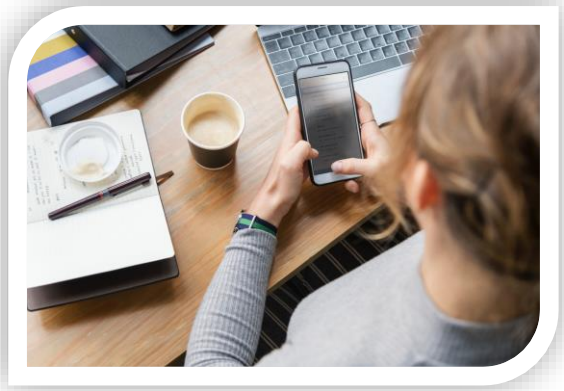
VAD ÄR EN PERSONUPPGIFT?

- All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

BEHANDLING AV PERSONUPPGIFTER

- En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter.

Exempel:
-insamling/framtagning
-sammanställning/organisering/strukturering/bearbetning
-ändring
-användning
-spridning
-lagring
-förstöring



KÄNSLIGA PERSONUPPGIFTER

- Ras och etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Hälsa och sexualliv
- Genetiska/biometriska uppgifter

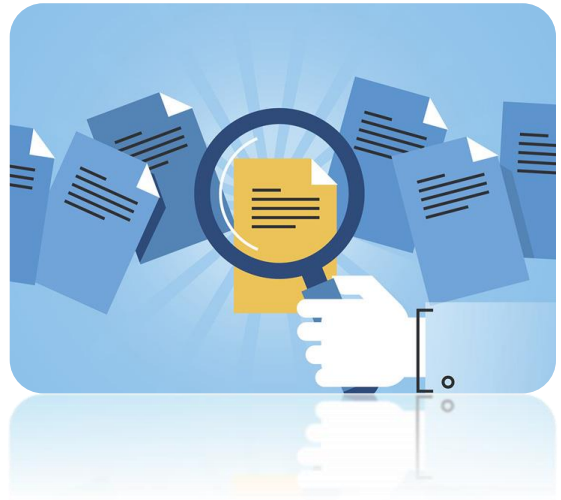
GDPR – TILLÄMPNINGSOMRÅDEN

Materiellt tillämpningsområde:

- Alla digitala personuppgiftsbehandlingar
- Alla personuppgifter som ingår (eller kommer att ingå) i ett register

Geografiskt tillämpningsområde:

- Alla personuppgiftsbehandlingar om personer som upprätthåller sig i EU.
- Alla personuppgiftsbehandlingar som utförs av en organisation som är etablerad i EU.



PERSONUPPGIFTSANSVAR - WEBBPLATSER

- Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till.
- Ägaren av webbplatsen är i regel personuppgiftsansvarig.
- Personuppgiftsansvarig ska tillse att bestämmelserna i GDPR efterlevs, ex. för de uppgifter som behandlas i kakor.
- Ansvaret gäller även om kakorna inte ägs av webbplatsen utan är tredjepartskakor från t.ex. Google Analytics, Facebook-pixel, AddThis, osv.

GDPR - GRUNDLÄGGANDE PRINCIPER

PRINCIP:	SKYLDIGHET FÖR PERSONUPPGIFTSANSVARIG:
• Laglighet	- Rättslig grund. Rättvis, skälig, rimlig och proportionerlig behandling.
• Ändamålsbegränsning	- Endast uttryckligt angivna konkreta och berättigade ändamål.
• Uppgiftsminimering	- Enbart behandla de uppgifter som är nödvändiga för ändamålen.
• Riktighet	- Uppgifter ska vara riktiga och, om nödvändigt, uppdaterade.
• Lagringsminimering	- Uppgifter får enbart sparas så länge de behövs för ändamålet.
• Integritet och konfidentialitet	- Vidta adekvata skyddsåtgärder, tekniska och organisatoriska.
• Ansvarsskyldighet	- Kunna visa att principerna efterlevs, genom dokumentation.

LAGLIGHET - RÄTTSLIG GRUND

Rättsliga grunder	Myndigheter	Privata företag
• Samtycke	N	J
• Avtal	J	J
• Intresseavvägning	N	J
• Rättslig förpliktelse	J	J
• Myndighetsutövning	J	(N)

REGISTRERADES RÄTTIGHETER

Du måste ange en kontaktväg för registrerade som vill utöva sina rättigheter

- Rätt till information
- Rätt till tillgång
- Rätt till rättelse
- Rätt till radering
- Rätt till begränsning
- Rätt att göra invändningar
- Rätt till dataportabilitet

DEL 2 – E-DIREKTIVET OCH KAKOR

E-DIREKTIVET

- EU-reglering av behandling av personuppgifter och integritetsskydd för elektronisk kommunikation

- E-direktivet gäller parallellt med GDPR

E-DIREKTIVET OCH KAKOR

- EU-direktiv om integritet och elektronisk kommunikation

- I Sverige omsatt till: **Lag (2003:389) om elektronisk kommunikation**

”6 kap 18 § Uppgifter får lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Detta hindrar inte sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst som användaren eller abonnenten uttryckligen har begärt.”

RÄTTSPRAXIS – EU-DOMSTOLEN

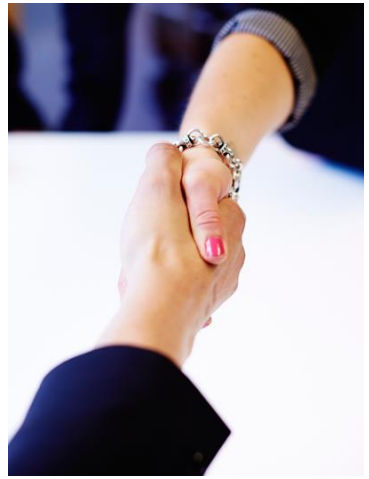
- EU-domstolen slår fast att användning av cookies kräver ett **aktivt** samtycke från webbplatsbesökare (dom i mål C-673/17, 1-10-2019).

- En på förhand ikryssad ruta räcker inte.

- Domen 2019 innebär att de flesta webbplatser behöver se över hur de hämtar in webbplatsbesökares samtycke för cookies som används för analysverktyg, marknadsföring, reklamnätverk och andra ändamål.

SAMTYCKE (GDPR OCH E-DIREKTIVET)

- Den rättsliga grunden samtycke innebär att den registrerade har sagt ja till personuppgiftsbehandlingen
- Den som samtycker måste informeras om personuppgiftsbehandlingen
- Samtycke måste vara frivilligt och jämlikt
- Med frivilligt menas att den registrerade har ett genuint fritt val och kontroll över sina personuppgifter
  - Samtycket måste t.ex. kunna återtas varefter personuppgifter måste raderas
  - Den registrerade får inte drabbas av negativa konsekvenser om den inte lämnar sitt samtycke, t.ex. nekas tillträde eller åtkomst till innehåll på en webbsida.



VIKTIGT ATT TÄNKA PÅ - KAKOR

Utforma en popup-banner för samtycke till kakor för webbplatsen:

- blockera kakor innan samtycke
- ge besökarna möjligheten att neka alla ej tekniskt nödvändiga kakor
- informera användare om webbplatsens användning av kakor
  - Syfte/ändamål, rättslig grund, mm.
- respektera användares integritetsval
- lagra dokumentation om samtycke i 5 år, enligt lagstadgade krav

Reglerna gäller inte bara för vanliga kakor utan även för annan jämförbar teknik som Tracking Pixels, Flash-kakor, html5 local storage, osv.

KONTROLLERA DIN WEBBPLATS

Webbkoll:

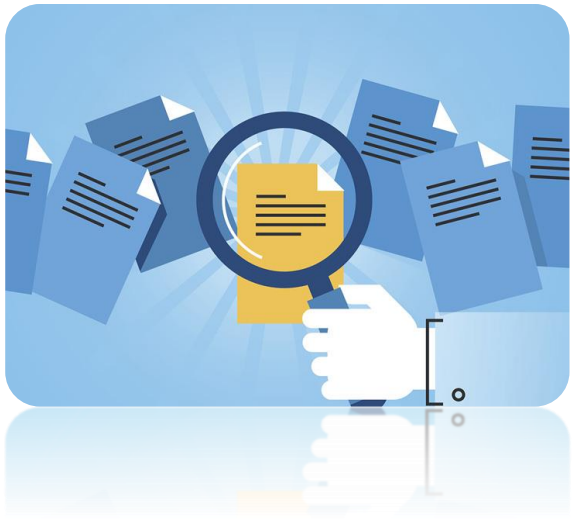
- https://dataskydd.net/webbkoll/
- Testa din webbsida!
- Åtgärda eventuella brister.

Webbkoll är ett analysverktyg för att undersöka dataskyddet på en webbplats. Verktyget ger konkreta tips och instruktioner för att åtgärda de problem som hittas.

QA OM COOKIES

- - Måste en användare samtycka till användandet av alla olika sorters kakor (temporära/sessionsknutna, långlivade, etc.)?
  - Får man använda kakor innan användaren har samtyckt/nekat till användande av kakor?
  - Vad behövs för att få en användares samtycke att använda kakor?
  - Hur styrker man att en användare har givit sitt samtycke?
  - Vad för risker finns det med att använda kakor utan att användaren samtycker?
  - Är det OK att vägra användaren åtkomst till sidan om denne inte samtycker till kakor?
  - Vad behöver man tänka på om användare kan skapa konton och logga in på ens hemsida (då personuppgifter sparas)?
  - Om användare kan skicka in något anonymt (t.ex. gästboksinlägg), påverkas det av GDPR på något vis? Även om det inte kan knytas till en specifik individ?

FÖRSLAG PÅ RESURSER



- www.integritetsmyndigheten.se
- https://www.pts.se/sv/privat/internet/integritet/kakor-cookies/
- https://dataskydd.net/
- https://webbkoll.dataskydd.net/sv/
- https://webbriktlinjer.se/riktlinjer/20-upplys-hur-juridisk-information-och-kakor-hanteras/
- https://cookieinformation.com/sv/vad-ar-reglerna-for-cookies/
- https://cookieinformation.com/sv/resurser/blog-sv/varfor-bor-ni-samla-in-samtycke-till-cookies/

FRÅGOR

JÖNKÖPING UNIVERSITY