1 Sammanställning av oönskade händelser

Sammanställning av gruppdiskussionen fån seminariet 7 oktober 2020 med Skolans personuppgiftshantering för att möta GDPR:s krav.

Frågor:

1. Vilka oönskade händelser/situationer ser ni finns med skolans hantering av personuppgifter?
2. Vilka ”Hotkategorier” kan de identifierade oönskade händelsen/situationen sorteras in under?

1.1 Sekretess

- Att känsliga uppgifter ska "läcka" ut.
- Skyddade identiteter läcker
- Värsta som kan hända att elever med skyddad identitet exponeras.
- Spridning till obehöriga
- Personer blandas samman
- Information skickas till fel elever när det finns flera med samma för- och efternamn
- Mejl som skickas till fel person som innehåller PU
- Elever livesänder.
- Risk att bilder och uppgifter klipps ut och används av andra
- Ett glömt papper i en skrivare som innehåller personuppgifter
- Brister i åtkomstkontrollen i tjänst leder till att personuppgifter läcks till användare som inte har autentiserat sig med tillräckligt (2fa). T.ex. en elev får åtkomst till känsliga personuppgifter med användarnamn och lösenord i en tjänst om den ligger på öppet nät).

1.2 Korrekthet

- Största risken är att elever kommer åt/ändrar uppgifter om varandra.

1.3 Tillgänglighet

1.4 Spårbarhet

1.5 Diverse

- Elever utsätts för direktreklam

Kommentar:

Generellt fokus på sekretess, att information sprids till obehörig. Frågan om korrekthet, tillgänglighet och spårbarhet ges lite eller ingen uppmärksamhet! År detta på grund av att det är mindre intressant, för att insikten saknas eller stort fokus på GDPR:s krav?

2 Sammanställning av orsaker till oönskade händelser

Då det var självklart för deltagarna att den oönskade händelsen är sekretess, kom gruppernas analyser snarare att handla om till varför orsaker uppgifter "läcker" ut. Dessa presenteras nedan.

2.1 IT-utrusning

2.1.1 Stöld

- Stöld av datorer etc – risk att lösenordet sprids.
- Vid ett inbrott där IT-utrustning stjäls kan känslig information känslig komma ut.
- Förlust/inbrott av utrustning med känslig information.
- Inbrott, stöld

2.1.2 Avyttring

- Slänger, kasserar hårdvara men har inte rensat ordentligt

2.1.3 Intrång

- Intrång i våra system.

2.2 Medarbetare

- Mänskliga faktorn är största risken. Inte medveten om saker man inte har kunskap om!

2.2.1 Acceptans

- Ej förankrat i organisationen
- Överdriven fråga
- Man gör som man vill.

2.2.2 Bristande kunskap/Medvetandegörande

- Tid att arbeta med frågan
- Nå ut i organisationen
- Det är lätt för lärare att "göra" fel och registrera sig och sina elever för gratis tjänster/programvaror. Stort problem i våras när många leverantörer erbjöd gratis...
- Användare kan inte tekniken
- Användare som inte har kunskap vad de får göra: Screen capture, skickar data via email etc.
- Osäkerhet gör att uppgifter lämnas ut godtyckligt
- Känslig info och för mycket info sparas och delas via moln eller mejl eftersom ”ingen ska ju in i min dator”. Ser den egna datorn som tillräckligt skydd.
- Rädsla för att göra fel gör att man håller för hårt i handlingar, vilket också kan vara fel
- Personal är inte medveten om vad som utgör personuppgift.
- Skolan uppdaterar inte regelbundet tidigare personal och inte ny personal i frågan.
- Pedagogens erfarenhet/hantering av PU

2.2.3 Handhavandefel

- Papper med personuppgifter
- Samma lösen till alla tjänster

- Säker utskrift
- Att eleverna får tillgång till ett personalkonto i klassrummet, vilket i sin tur kan leda till oönskade personer får tillgång till vissa uppgifter.
- Om inte pedagog loggar ur från sitt system, så kan obehörig gå in och ändra t ex bedömningar.
- Extern lagring - Sparar elevuppgifter på fel plats ex usb eller lokalt på dator (kan ex bli stulna).

2.3 Ledning/resurser

2.3.1 Resurser/prioritering

- Chefer som inte sätter av tid för personal att få tillräcklig tid att ta in all kunskap som behövs resulterar i okunskap bland personal.
- Uppskattar inte kostnaden när man går till molntjänst, omfördelning av resurser. Utbildning behövs av ledningen.
- Personuppgiftsansvarig lägger endast resurser på de stora dragen i lagstiftningen och inte till det praktiska arbetet i arbetsrum och lektionssalar.
- Inga resurser för risk och konsekvensbedömning ges.
- Arbetet hinns inte med.

2.3.2 Juridik/Oklart rättsläge

- PU-hantering kompliceras av andra lagar med krav på lagring.

2.3.3 Policy

- Risken kontra allmän handling, vad kan lämnas ut kontra vad ska lämnas ut?
- Ansvaret är hos användaren och inte hos leverantören.

2.4 Rutiner

- Rutiner som är tydliga
- Stöd uppifrån till verksamheten
- Skolorna glömmer meddela när elever slutar/flyttar.
- Kommuner och skolor som överför elevdokumentation mellan skolor via mail.
- Gallringsplaner saknas hos många av våra kunder.
- Problem med rutinerna för elever med sekretessmarkering, speciellt vid överföring mellan system.
- Telefonnummer och e-postadresser blir inaktuella, vilket leder till att utskick kan gå till fel mottagare.
- Uppkopierade listor på papper för snabb tillgång om/när man kanske behöver
- Fel uppgifter eller inaktuella mallar för allmänna offentliga handlingar ger för mycket info när de lämnas ut. T.ex. känsliga uppgifter skrivs in i ett ÅP, alltid fullt personnummer på betygskataloger osv
- De jämför med andra kommuner som godkänt (men de får ju…)
- Olika kommuner gör olika
- Metodik är inte utarbetad.

- I händelsen av att arbetet med personuppgifter inte är levande eller att det faller mellan stolarna så tappas kontroll.

2.4.1 Underhåll av masterdata/grunddata

- Att vi sitter på en massa gamla uppgifter.
- Uppgiftsminimering som inte borde sparas.
- Ej aktuella användare tas inte bort ur system. Uppgifter som mejl och skolbehörighet uppdateras inte i system.

2.5 Sociala medier

- Att skolor tycker det är OK att kommunicera med bilder via sociala medier.
- Info om elever sprids på sociala medier
- Lockas att använda sociala medier.
- Att använda applikationer som inte är anpassade för skolan.

2.6 E-post

- Dela uppgifter mellan verksamhet och förvaltning eller inom verksamhet
- Osäker typ av kommunikationssätt, mejl för snabbhet
- Oriktig hantering av känsliga personuppgifter – läkarintyg mejlas
- Onödigt mycket information går via mail.
- Onödig spridning av personuppgifter i mejlkonversationer.
- Att data kommer i fel händer är stor med mejl.
- Hur ska jag veta att det verkligen är den person jag pratar med?
- Hur ska jag veta att ingen annan tar del av infon? Tänker också att det är lätt att uppgifter/foton/klasslistor mm sparas lite här och där både lokalt o på olika mappar på server.
- Att personer inte veta vad som är /inte är personuppgift.
- Mejl - ostrukturerad information, hantering i stuprör, olika per förvaltning.

2.7 Tekniska brister

2.7.1 Tekniska brister

- Möjlighet till spårbarhet saknas
- Att uppgifter syns i ett verksamhetssystem för personer som normalt inte skall ha behörighet att se dessa

2.7.2 Behörighetshantering

- Lätt sökbara uppgifter i ett AD där vem som helst som har ett konto i kommunen kan söka på elever och hemvist
- Risk att någon har för hög behörighet
- System där man kommer åt mer information än vad som krävs för arbetet.

2.7.3 Bristande integrationer

- Sekretessbelagda elever lättare att hantera manuellt
- Manuell hantering
- Fördröjning i lärares idé och behov gör att man struntar i korrekt hantering, eller verksamheten blir lidande
- Skolans adminpersonal kan inte själv ta bort elever. Måste kontakta leverantören

2.8 Hantering av appar och tjänster

- Möjligt att registrera sig på alla möjliga tjänster
- Communities med tjänster utan tydlig ägare
- Många pedagogiska verktyg och appar är mycket lättillgängliga, vilket är positiv ur pedagogiskt perspektiv men inte i ett integritetsperspektiv.
- Det är enkelt att använda en digital system/tjänster - risk för olaglig behandling av personuppgifter.
- Handhavandefel anser vi är största risken med behandlingen. Att personal använder icke testad programvara.

2.8.1 Granskning

- Granskning och hantering av appar- tidskrävande och svårt.
- Upplevs som en bromskloss i utvecklingen att behöva granska.
- Svårt genomföra appgranskning och utreda var information lagras /skickas.

2.8.2 Lärares hantering

- Lärare som testar ett nytt digitalt läromedel och lägger in sin klass i detta.
- Lärare/fsk lärare använder appar och program utan godkänt PUB avtal och med hänsyn till GDPR - speciellt om andra huvudmän/ skolor/kommuner ansett dem godkända. Ett tydligare ramverk behövs för att vi skall tolka på samma sätt.
- Personal använder appar utan att de förstår att dessa delar personuppgifter.
- Ambitiösa och kreativa lärare som hittar gratisverktyg på nätet och kopplar elevkonton dit.

2.8.3 Elevers hantering

- Moderna digitala verktyg som eleverna använder för att göra en film eller en podd som skickas ut till vårdnadshavarna.
- Elever använder appar/tillägg (vi har Chromebooks och arbetar i Google) som innebär en säkerhetsrisk. Ex appar/tillägg som livesänder. Hur löses det i skolorna? Vi spärrar regelbundet men det är svårt att följa utvecklingen.

2.9 Externa organisationer/leverantörer

- Hantering av PU i tredjepartssystem med integrationer till andra tjänster. Många roller och vyer i systemet
- Kontrollera fel utifrån, ex. tjänsteleverantörer.
- Tillit till utomståendes hantering

2.9.1 PUB-avtal

- Skolans personuppgifter ”delas” till många. Vi måste säkerställa att leverantörerna efterlever PUB-avtalet. Exempel, att det raderas när det ska

2.9.2 Intrång

- Intrång i våra leverantörers system.

2.9.3 Molntjänster

- Det finns en osäkerhet vid användning av molntjänster, var hamnar datan och hur säkert är det?
- Att uppgifter sparas på ställen som inte är lämpliga "USA" (t ex Schrems II)
- Att känsliga uppgifter oavsiktligt delas tex. i molnet. Kan leda till att personer som inte ska ha tillgång till dessa får det.
- Office365 och GSuite tredjeland
- Molnplattformar – Informationsöverskott

---

3 Lösningar

3.1 Teknik

- API:er skulle underlätta. Konsensus för API:er. Att data finns på ställen som inte är övergripbara (okontrollerad spridning) från användaren (elevens).
- Onödigt mycket information överförs om elever till olika molnleverantörer och läromedelsleverantörer. Vore bra att i större mån kunna pseudomymisera uppgifter i högre grad, ex vid federationslösningar och liknande.

3.2 Integrationer

- Att inte skapa användare i system som hanterar läromedel utan göra en koppling med integration som ex Skolfederationen där användare automatiskt uppdateras blir det lättare att säkerställa att inte fel uppgifter ligger på användare eller att användare ligger fel.

3.3 Autentisering

- Säker inloggning för personal och elever (stark autentisering)
- Federationsinloggning för skolans personal och elever, till lärplattformer och andra syst

3.4 Medvetandegörande

- Utmaning att öka medvetenheten hos personalen