

GDPR anpassningar i TYRA

Vi har utformat både plattformen och våra avtal så att de är helt GDPR anpassade. För fullständiga villkor så hänvisar vi till vårt PUB-avtal och vårt användaravtal. Här följer en förkortad och förenklad version av vår policy om GDPR och hur vi anpassat plattformen till GDPR.

Hantering av er data.

Först och främst, ni (verksamheten) äger all er data. Vi är verksamhetens biträden. Hur vi hanterar data, var den sparas och vad ert respektive vårt ansvar är definieras i det PUB-avtal (PersonUppgiftsBiträdesavtal) som vi skriver med er.

Innan ni kan börja använda TYRA i er verksamhet krävs ett sådant avtal.

Samtycken och Användaravtal måste uttryckligen ges av användarna i samband med att de skapar sina användare i TYRA.

Dessa är skrivet på ett enkelt och förståeligt sätt. Men i de fall där det behövs förtydligande har vi även lagt in det. T.ex att man är införstådd i hur fritextfält får användas och att om man lägger in egna kontakter så behövs det nu även samtycke från dem.

Dessa villkor och avtal finns lättillgängliga i TYRA så att användaren närsomhelst kan gå tillbaka och läsa dessa.

Varje personuppgiftsbehandling sker enligt följande principer:

- Laglighet
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet

I korta drag betyder det att vi samlar bara in och lagrar de uppgifter som behövs för att verksamheten på förskolorna ska fungera på ett tryggt och säkert sätt.

Om en användare raderar sig kan de t.ex välja om de vill bli helt raderade och anonymiserade eller bara radera sina personuppgifter, men t.ex låta för- och efternamn stå kvar i kommentarer och poster. Mer om detta är beskrivet i PUB-avtalet.

Hela systemet skyddas med TLS som hanterar datan så att den är krypterad och säker. TLS hette tidigare SSL men istället för att kalla det SSL 3.0 så bytte man till TLS.

https://sv.wikipedia.org/wiki/Transport_Layer_Security

Uppgifterna i TYRA är endast till för verksamheten och vi följer hela tiden de instruktioner som lämnas av verksamheten avseende hanteringen av uppgifterna, exempelvis gällande radering, begränsningar osv.

Bayou använder sig av en underleverantör, Elastx, för förvaring av data i Tyra. Elastx uppfyller EU:s krav på behandling av personuppgifter.

Elastx (<https://elastx.se/>) server ligger i Stockholm. De har en ISO27001 certifiering.

För en publik version om deras säkerhetspolicy, se

<https://elastx.se/en/information-security-policy>. De har även en årlig audit gällande ISO27001.

I de fall som en underleverantör anlitas så ingås ett underbiträdesavtal mellan underbiträdet och oss innehållandes motsvarande skyldigheter som detta personuppgiftsbiträdesavtal.

Praktiska punkter i TYRA som vi gjort för att anpassa oss till GDPR

- Helt nytt sätt att bjuda in användare, istället blir det en inbjudan via ett mobilnummer och sms verifikation. Även kallat 2-faktorsinloggning. Inbjudan hanteras av Admin på verksamheten.
- Olika nivåer på personalbehörighet.
 - Nivå 1: Full behörighet.
 - Nivå 2: Begränsad behörighet (inte se känslig persondata så som personnummer, allergier, anteckningar osv)
- Det kommer nu även krävas samtycke för att lägga till ytterligare kontakter i TYRA.
- Uppdaterade avtal samt en del förtydliganden för t.ex fritextfält mm
- Användare kan nu radera sig själva på ett enkelt sätt. I samband med detta så kan man välja huruvida man vill anonymisera sina uppgifter eller inte (dvs om man t.ex gjort ett inlägg i Bloggen så kan man alltså välja att låta sitt för- och efternamn stå kvar som "postare").
- Vi loggar även ändringar som gjorts och av vem i "Allergi och övrig info" på barnets profil. Denna information kan vi då ta fram på begäran från ansvarigt dataskyddsombud.
- Har man redan skapat en användare via email så går det nu att konvertera till 2-faktor med sms, vilket vi starkt rekommenderar, så får man gå till sina inställningar och trycka på "Konvertera till sms inlogg". Då kommer man slippa lösenord via verifikationsmail.