GDPR

En nulägesbild av Nova Softwares arbete med GDPR

GDPR – General Data Protection Regulation – *dataskyddsförordningen*

Dokumentinformation	
Författare (alt. ansvarig)	Nova Software Dataskyddsgrupp
Version	1.0
Senaste uppdaterad	2017-12-06

Förord

GDPR (General Data Protection Regulation – eller *dataskyddsförordningen*) syftar primärt till att stärka rättigheter för den enskilde när det gäller *personlig integritet*. Från och med 25 maj 2018 gäller GDPR som lag i EU:s medlemsländer. GDPR ersätter tidigare Personuppgiftslagen (PuL).

- Centralt i GDPR: ett **ökat ansvar** för den som behandlar **personuppgifter**

Nova Software har utfört en förstudie kopplat till GDPR. Förstudien syftade till att genomföra en programvaruinventering (identifiera programobjekt vilka behandlar personuppgifter) samt att identifiera och upprätta en förteckning över övriga centrala områden som berörs av GDPR.

Arbete med GDPR fortsätter i projektarbetsform fram till 25 Maj 2018, för att därefter fortsätta i förvaltningsform. Detta dokument fokuserar mot vår kärnprodukt Skola24[1] och två för ändamålet nödvändiga kringsystem (Lime och Visma) – dvs. dokumentet redogör inte för samtliga de system som identifierats, vilka i någon form behandlar personuppgifter vid Nova Software.

Syftet är att bistå med en övergripande informationsinsats runt hur Nova Software ser på, och förhåller sig till GDPR, för att därigenom försöka underlätta för våra kunder och deras arbete.

I dokumentet förekommer information om begrepp, innebörd och förhållningssätt. *Det bedöms viktigt att framföra att den information som förmedlas, grundar sig på hur Nova Software ”tolkat” begrepp och dess innebörd, för att därigenom anta ett förhållningssätt.*

Ambitionen är att bistå kund (och personuppgiftsansvarig) *med stöd kring hur Skola24 och dess behandling kan motiveras, information avseende hur Nova Software tolkar inslag i GDPR samt att försöka svara upp mot vanliga frågor (i egenskap av Personuppgiftsbiträde).*

Om du har ytterligare frågor kring Skola24 och GDPR

- Befintlig kund, vänligen kontakta Kundansvarig
- Ej befintlig kund, vänligen skicka ett mail till info@novasoftware.se

I fall där din första kontaktpart inte kan besvara en fråga kommer nödvändiga medarbetare inom Nova Software att kontaktas för att försöka hjälpa dig med dina funderingar.

I dokumentet förekommer hänvisningar till utredningar. *Med utredningar avses att det finns en pågående eller planerad kontakt med juridisk kompetens, en planerad eller pågående informationsinhämtning från Datainspektionen, alternativt en intern utredning.*

Tänk slutligen på att detta är en nulägesbild av Nova Softwares arbete med GDPR. Om du tar del av dokumentet, är det viktigt att du är medveten om att det över tid kan komma att uppdateras[2].

Grundläggande referenser till detta dokument

- Datainspektionen
  - Länk – PuL
  - Länk – GDPR
- Skolverket
  - Länk – Skollagen

Det känns inledningsvis också viktigt att påpeka, att oavsett om det finns mycket nyheter med GDPR, så finns det också mycket som i princip är oförändrat i förhållande till PuL.

[1] Dokumentet kommer även att redogöra för Novachem – föregångaren till Skola24 Schema.
[2] En uppdatering kan vara ett resultat av en utbildning inom området eller ett resultat av en pågående utredning inom området.

FAQ och referens

Nedan presenteras ett antal frågeställningar om GDPR som bedöms vanligt förekommande mot Nova Software för tillfället, och en referens till var i dokumentet information kan hittas.

Tabell 1: FAQ

Fråga	Kapitel
Kan ni redogöra för syftet med den persondatabehandling ni utför?	2.1
Kan jag som lärare få fram vilken persondata som lagras om mig?	2.1
Hur ser ni på gallring av personuppgifter?	2.11
Hur ser ni på begreppet ”dataportabilitet”?	2.8
Varför används personnummer i Skola24?	2.4
Hur ser ni på samtycke runt den behandling som utförs?	2.2, 2.10
Vem/vilka arbetar med GDPR inom er verksamhet?	3.3
Hur ser ni på begreppet ”Privacy by design”?	2.6, 3.2
Kan föräldrar se frånvaro även när en elev fyllt 18?	2.10
Behandlar ni ”känsliga personuppgifter”?	2.3, 3.5
Kan ni redogöra för var ni lagrar data om våran kommun?	2.12

Innehåll

1 Avtalshantering 4

2 Skola24 översikt 5

2.1 Syfte (ändamål) 5

2.2 Rättslig grund 5

2.3 Personuppgifter 6

2.4 Personnummer 7

2.5 Roller och konto 7

2.6 Inbyggd integritet 7

2.7 Informationsflöde 8

2.8 Uttag av data 8

2.9 Rättning av data 9

2.10 Specifik åtkomst 9

2.11 Gallring och lagring 9

2.12 Lagringsplats (datacenter) 10

3 Övrig information 11

3.1 Skyddsklassning 11

3.2 Dataskyddspolicy 11

3.3 Dataskyddsgrupp 11

3.4 Rapportering 12

3.5 Nova Excellence 12

4 Nödvändiga kringsystem 13

5 Versionshistorik 14

1 Avtalshantering

I samband med införande av Skola24 upprättas ett avtal mellan Nova Software och en kund. Detta avtal reglerar enkelt beskrivet kundens rätt, att under en given period använda ett system som har utvecklats av Nova Software AB, såväl som vilka skyldigheter och rättigheter dessa parter har.

För att framföra exempel på vad som driver utveckling av funktionalitet i Skola24, så kan *offentliga upphandlingar* nämnas. För att det ska finnas ett intresse för en kommun att teckna ett avtal med Nova Software, så *bör* eller *skall* viss funktionalitet också kunna representeras i Skola24.

Ovan är också anledningen till att vi ibland resonerar om ”kunddriven utveckling”.

Nova Software agerar vidare som Personuppgiftsbiträde (för en skola/kommun). Detta innebär att behandling av personuppgifter i Skola24, utförs på uppdrag av en Personuppgiftsansvarig (dvs. på uppdrag av en skola/kommun) – *behandling utförs för den personuppgiftansvariges räkning.*

Ett Personuppgiftsbiträdesavtal (PUB-avtal) upprättas mellan *ansvarig* och dennes *biträde.*

För att framföra exempel på ingående reglering i ett personuppgiftsbiträdesavtal, så kan det vara att Nova Software som biträde ska förhålla sig till *tystnadsplikt* vid behandling av personuppgifter såväl som att säkerställa att lämpliga *säkerhetsåtgärder för dataskydd* vidtas.

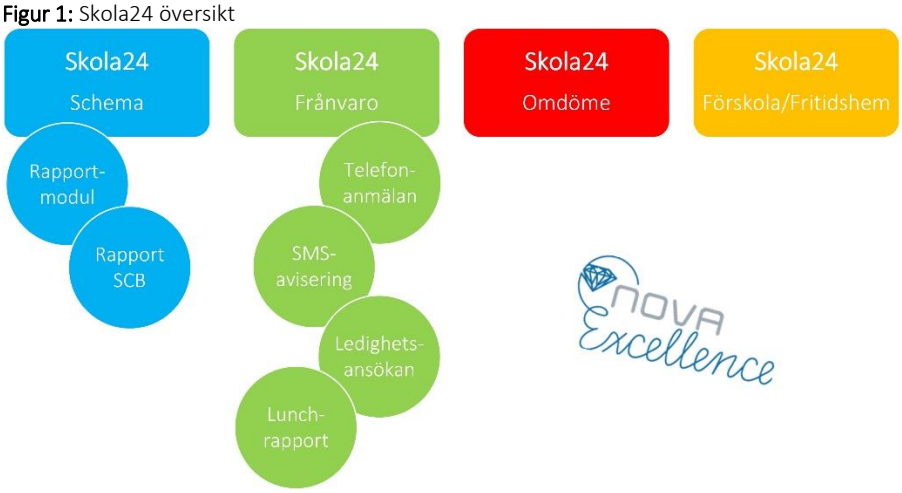
Det anses här av relevans att framföra att tystnadsplikt ingår i samtliga anställningsavtal vid Nova Software. Däremot genomförs en utredning för att genomlysa befintliga formuleringar. När det kommer till *säkerhetsåtgärder för dataskydd*, så redogörs detta senare i dokumentet.

2 Skola24 översikt

Skola24 kan enkelt beskrivet uttryckas som en *webbtjänst* (*webbapplikation*) – programvara vilken användare kommer åt med hjälp av en webbläsare.

Skola24 struktureras med hjälp av *funktionsområden*, vilka kan kompletteras med olika *tillval*. Nova Software erbjuder även *kurs- och konsultverksamhet* runt Skola24 – Nova Excellence.

Figur 1: Skola24 översikt



För mer information om Skola24 och Nova Excellence, se novasoftware.se.

2.1 SYFTE (ÄNDAMÅL)

Syftet med den personuppgiftsbehandling som utförs i Skola24 är att underlätta för en huvudman att kunna bedriva sin skolverksamhet (i enlighet med Skollagen såväl som övriga förordningar och föreskrifter från Skolverket). Syftet är helt enkelt att underlätta för skolans verksamhet genom att tillhandahålla funktioner som utgår från skolans behov (eller krav) – se Figur 1.

Nova Software utreder för tillfället ett framtida tillförande av en ”dataskyddsöversikt”. Som namnet antyder, är också tanken att det ska vara en övergripande funktion. Det skulle kunna handla om en funktion som aktiveras om behov finns (från skolan/kommunen), för att möjliggöra för våra kunder att i sin tur informera användare av Skola24 om vilka personuppgifter som behandlas, och för vilket ändamål. Nova Software skulle om möjligt också kunna bistå med att ta fram en standardtext kring ändamålet utifrån de olika roller som finns, men där det också erbjuds en *redigeringsmöjlighet*.

Exempel: en vårdnadshavare önskar veta vilka personuppgifter som behandlas för sitt barn. Vårdnadshavaren loggar in i Skola24, letar upp ”dataskyddsöversikt”, för att på så sätt få fram vilka uppgifter som behandlas, och för vilket ändamål. Samma upplägg är giltig även för övriga roller – så som i fall där en lärare önskar motsvarande information.

Senare delar av dokumentet kommer också återkomma till tankar med en ”dataskyddsöversikt”.

2.2 RÄTTSLIG GRUND

Inom GDPR är en central aspekt vid behandling av personuppgifter att identifiera en *rättslig grund*. För att det ska vara tillåtet att behandla personuppgifter, måste det finnas stöd utifrån GDPR.

Nedan presenteras exempel på villkor som kan härledas till en rättslig grund för behandling;

1. Behandlingen är nödvändig för att fullgöra en **rättslig förpliktelse**
    a. Det finns en laglig grund den behandling som utförs
2. Behandlingen är nödvändig för att **fullgöra ett avtal**
    a. Avtal Kund <> Leverantör
3. Behandlingen är nödvändig för ett **berättigat intresse**
    a. Det är möjligt att stödja behandling på en intresseavvägning
4. Behandlingen är förankrad i ett **samtycke för behandling**
    a. Användare samtycker till den behandling som utförs

Den personuppgiftsbehandling som utförs i Skola24 bedöms huvudsakligen vara motiverad genom en rättslig förpliktelse (Punkt 1). Bedömningen är behandlingen i stor omfattning motiveras med stöd av Skollagen och/eller övriga förordningar och föreskrifter från Skolverket.

Exempel: enligt Skollagen, så ska ogiltig frånvaro för ej myndiga elever rapporterats till vårdnadshavare samma dag som frånvarotillfället ägt rum. För att möjliggöra denna insats, är det helt avgörande att behandla vissa personuppgifter, för att därigenom kunna informera vårdnadshavare om en sådan händelse med hjälp av ett systemstöd.

Att det finns ett *syfte (ändamål)* med den behandling av personuppgifter som utförs (ref. 2.1 Syfte (ändamål)) i kombination med att en *rättslig grund* är identifierad är en grundförutsättning – HUR personuppgifter vidare behandlas, kan då initialt förankras mot centrala kriterier inom GDPR. I fall av förändringsbehov, kan dessa grundförutsättningar också kontrolleras innan förändringsbeslut.

Ovan räcker naturligtvis inte för att uppfylla GDPR. Behandlingen av personuppgifter ska även uppfylla de övriga bestämmelser som finns i förordningen, där ansvariga parter även ska kunna redogöra för sin uppfyllnad. Utvalda villkor/aspekter, kommer redogöras i senare delar av dokumentet.

2.3 PERSONUPPGIFTER

Den typ av personuppgifter som behandlas i Skola24, utgörs i huvudsak av personnummer, namn och kontaktuppgifter. Det handlar exempelvis om förnamn, efternamn, telefon och e-post.

Skola24 är sitt grundutförande inte utvecklat för att behandla *känsliga personuppgifter,* så som behandling av data som rör politiska åsikter, religiös övertygelse eller uppgifter om hälsa.

Ett undantag kan vara att Skola24 behandlar data som berör modersmålsundervisning. Denna typ av data kan klassificeras som känslig i viss mån med anledning av dess koppling till *etnicitet*.

Exempel: i Skola24 Schema (inkl. Novaschem) är det möjligt att schemalägga lektioner för elever som ska undervisas i ett modersmål. I Skola24 Frånvaro kan Frånvaro/Närvaro hanteras till modersmålsundervisningen. Det finns därigenom viss behandling av personuppgifter som kan uttryckas som behandling av *känsliga personuppgifter*.

Att modersmålsundervisning behandlas i Skola24 motiveras dock utifrån Skollagen – dvs. det finns en laglig grund (ref. 2.2 Rättslig grund). Däremot utreds för närvarande om exponering av viss data kan vara nödvändig att koppla till begränsningar. Det kan till exempel handla om införande av ett tekniskt stöd som kan användas om det anses nödvändigt, vilket skulle fungera som ett regelverk för våra kunder när det kommer till hantering av åtkomst till schema på elevnivå.

2.4 PERSONNUMMER

Till att börja med anses personnummer vara det *enskilda attribut* som *idag* lämpligast används för att unikt identifiera en person (i den kontext som Nova Software verkar). Personnummer är heller inte förändringsbenägna; jämför namn, e-post, telefonnummer etc. Att utfärdande och underhåll hanteras av en myndighet (Skatteverket), anses också bidra till en grundläggande trygghet.

Eftersom Skola24 (inkl. Novaschem) i flera fall samverkar med andra system för att utbyta data, så förekommer vanligtvis också en relation (integration) till ett *person- eller befolkningsregister*[3]. Det är därför avgörade att det också mellan dessa system finns en form av gemensam nämnare för att identifiera personer, för att därigenom kunna säkerställa övriga förhållanden som råder – vilket till exempel kan handla om förhållanden mellan elev > klass eller mellan elev > vårdnadshavare

I fall där *e-legitimation* efterfrågas i Skola24, anses det också viktigt att belysa att i flera fall är det nödvändigt att personnummer behandlas – exempelvis när BankID används för identifiering.

För att också härleda till ett syfte, så handlar det om att kunna identifiera personer med hjälp av en unik identitetsbeteckning samt om att kunna uppfylla krav på stöd för e-legitimation.

Att personnummer används för identifiering, anses kunna motiveras genom en intresseavvägning och hänvisning till ett berättigat intresse (ref. 2.2 Rättslig grund). För att utveckla – det anses vara nödvändigt för att kunna erbjuda ett tillförlitligt stöd vid identifiering av personer och relationer.

2.5 ROLLER OCH KONTO

Skola24 baseras på roller. Beroende på de funktioner som avtalats, finns roller för schemaläggare, elever, vårdnadshavare, lärare samt kanslister respektive skol- och kommunadministratörer.

Dessa roller har också ett konto (”användarkonto”). I grundutförandet används *användarnamn* och *lösenord* för åtkomst (1-faktorautentisering), men det är möjligt att utöka med en högre säkerhetsnivå om behov föreligger, så som i fall där 2faktorautentisering genom stöd för BankID önskas.

Med hjälp av användarroller, i kombination med underliggande relationer (exempelvis: elev > klass > lärare), begränsas också möjligheter till granskning och behandling av information. Att komma åt viss information om en elev, förutsätter exempelvis en given roll eller en utökad behörighet.

Ovan kan även härledas till det som GDPR omnämner som *säkerhetsåtgärder för dataskydd.*

2.6 INBYGGD INTEGRITET

I samband med GDPR lägger Nova Software stor vikt vid något som kallas för ”Privacy by design” – vilket enkelt uttryckt kan beskrivas som inbyggt dataskydd eller *inbyggd integritet*.

Inbyggd integritet kan handla om att tillämpa *uppgiftsminimering* – att enbart samla in/behandla de personuppgifter som är nödvändiga för ändamålet, såväl som om att säkerställa att de personuppgifter som behandlas, enbart används för det ändamål som avsågs vid tiden för insamling – vilket också kan vara exempel på inslag i ett personuppgiftsbiträdesavtal (ref. 1 Avtalshantering).

[3] Vid arbete med ”skolrelaterade system”, finns ofta en relation (integration) till ett *person- eller befolkningsregister* genom de system som används. Exempel: SPAR – Statens Person och AdressRegister (för företag), Navet (för myndigheter), KIR (KommunInvånarRegister).

Övriga aspekter kan handla om att tillse att det finns stöd för att säkerställa att åtkomst till personuppgifter begränsas till de personer som behöver det för att kunna utföra sina arbetsuppgifter.

Exempel: det är fullt möjligt att ”skall-krav” från en föreliggande upphandling mynnar ut i tillförande av ny funktionalitet i Skola24. I fall där personuppgifter behandlas, kan Nova Software tillse (understödja kravställaren) att funktionalitet som utvecklas, enbart behandlar nödvändiga personuppgifter samt att åtkomst regleras genom särskilda behörighetskrav.

2.7 INFORMATIONSFLÖDE

Skola24 (inkl. Novaschem) föds och underhålls (i huvudsak) med hjälp av integrationer mot ett s.k. ”elevregister” (men det är också möjligt att manuellt mata in information).

Utöver att Nova Software kontinuerligt försöker närvara i olika forum runt informationsflöde som rör dataöverföringar mellan ”skolrelaterade system”, så genomförs en intern utredning för att se över möjligheter att förbättra underhåll av specifika relationer, så som elev > vårdnadshavare.

Exempel: när data skickas mellan ett ”elevregister” och Skola24 (inkl. Novaschem) är det bl.a. information on elev (namn, personnummer), vårdnadshavare (namn, personnummer), klass, ämne och skola som behandlas.

I fall där en kund önskar arbeta med SSO (Single Sign-On) mot Skola24 kan ett tillval avropas. Detta tillval medför att persondata (så som personnummer) utbyts inom en s.k. federation, vilken i sin tur består av ett antal olika parter (till kund övriga leverantörer som är nödvändiga för federationen).

När det kommer till elevregister har en skola/kommun ett avtal med en leverantör av elevregister, såväl som ett avtal med Nova Software för att aktivera stöd för avsedda integrationer. Detta upplägg gäller även för SSO. Dvs. skolan/kommunen har ett avtal med två leverantörer för ändamålet.

Nova Softwares samverkansprogram syftar till att främja öppenhet mellan system och leverantörer i den skoladministrativa branschen. Det är möjligt att en kund önskar använda Skola24 Schema för schemaläggning och en annan produkt (leverantör) för frånvarohantering (eller annat ändamål).

Att Skola24 samverkar med en ”tredje part” regleras genom följande avtalsupplägg: Nova Software har ett aktivt avtal med en skola/kommun. Om skolan/kommunen önskar att leverantör NN ska få konsumera data från Skola24, upprättar skolan/kommunen ett avtal med leverantör NN vilket bl.a. redogör för vilken typ av personuppgiftsbehandling som avses. Leverantör NN tecknar också avtal med Nova Software (”samverkansavtal”) som bl.a. reglerar hur och när data kan konsumeras.

För ovan finns en form av ”treparts-avtal” (Kund > Leverantör A samt Kund > Leverantör B) för viss funktionsuppfyllnad. Det bedömning som görs, är att det (indirekt) finns avtal som ligger till grund för (dvs. reglerar) den personuppgiftsbehandling som utförs (ref. 2.2 Rättslig grund) – dvs. specifik personuppgiftsbehandling är nödvändig för att *fullgöra ett avtal*.

I de fall en kund arbetar med Skola24 Frånvaro och tjänsten *Frånvaroavisering via SMS*, genomförs viss persondatabehandling av en underleverantör till Nova Software (Cellcynt AB) – utskick av SMS. Det bedöms här viktigt att påvisa att en utredning genomförs för att se över rådande funktion och dess avtalsupplägg – vilket bl.a. avser utreda om vissa inslag av personuppgiftsbehandling kan vara nödvändiga att förtydliga i avtalet med underleverantören (genom dess underbiträdesavtal).

2.8 UTTAG AV DATA

Se inledningsvis 2.1 Syfte (ändamål) och ”dataskyddsöversikt”. Ett komplement till en övergripande

funktion för att överblicka personuppgiftsbehandling skulle kunna vara att erbjuda att ”grunddata” (*grundläggande personuppgifter*) även kan läsas ut i ett för ändamålet lämpligt dataformat. Detta skulle också kunna ses som en form av övergripande *registerutdrag* som tillhandahålls.

Att en användare kan få ut data i ett för ändamålet lämpligt dataformat, innebär också att det finns en möjlighet att använda grunddata på annat håll (GDPR – ”dataportabilitet”). Det känns här viktigt att belysa att den bedömning som Nova Software gör kring dataportabilitet, är att det övervägande handlar om främjande av standards vid *byte av tjänster* – så som när en privatperson byter bank.

Det är vidare viktigt att påpeka, att de detaljerade utdrag som efterfrågas från användare i Skola24, i flera fall kan hanteras genom *rapportmöjligheter* – vilket i viss mån också kan ses som en form av utökade *registerutdrag*. Det kan handla om att en skola/kommun betjänar ett frånvaroutdrag som efterfrågas från en vårdnadshavare. Det ska i sammanhanget också poängteras att Nova Software i egenskap av personuppgiftsbiträde ska bistå vid behandling mot en huvudman. Det kan handla om att omfattning eller komplexitet på ett uttag motiverar stöd från Nova Software.

Över tid är det fullt möjligt att det framkommer att ”särskilda datauttag” ofta efterfrågas, vilket i sin tur kan innebära en framtida kravställning mot Nova Software avseende uttag av data.

2.9 RÄTTNING AV DATA

Det är idag möjligt att förändra (rätta) persondata i Skola24, så som att en användare själv (genom användarkonto), eller med hjälp av en roll på en skola ändrar en e-postadress. Viss persondata kan även uppdateras från eventuella integrationer som finns till Skola24 (ref. 2.7 Informationsflöde).

2.10SPECIFIK ÅTKOMST

Det är idag möjligt att begränsa åtkomst till data i Skola24 – automatiskt respektive manuellt. Med automatisk begränsning avses bl.a. att när en elev blir myndig, så införs automatiska begränsningar i Skola24 som åsidosätter möjligheten att vårdnadshavare kan granska och behandla specifik data.

I fall där en elev önskar att vårdnadshavare fortsatt ska kunna granska data, så krävs ett samtycke från eleven, dvs. en aktiv insats för att aktivera att vårdnadshavare får sådan möjlighet. Detta kan idag hanteras genom att eleven framför sådant önskemål till en administratör som utför insatsen.

Det kan också handla om att ett användarkonto automatiskt upphör i och med avsaknad av skolplacering – vilket i sammanhanget kan likställas med avaktivering av användarkonto.

Med manuell begränsning avses bl.a. möjligheten att en administratör kan avaktivera användarkonto, så som vid upphörande av anställning (exempelvis då en lärare slutar).

Ovan utgår från ett läge där skolan/kommunen arbetar med användarkonto i Skola24.

2.11GALLRING OCH LAGRING

När det kommer till radering av persondata, är det viktigt att belysa att bl.a. Skollagen i specifika fall medför begränsningar avseende att data inte nödvändigtvis kan raderas.

Exempel: i GDPR finns en hel del information om radering av data (GDPR – ”rätten till radering”). En person kan upprätta kontakt med en systemleverantör och begära att persondata ska raderas. Det som är viktigt här är att det finns en medvetenhet om att det i flera fall finns lagar som överträder denna ”rätt”. Precis som att det inte går att begära att viss data raderas i ett Brottsregister, så går det inte att begära att viss data raderas i ett Frånvarosystem. Det finns en laglig grund.

Ovan ska dock inte tolkas som att det inte går att ta bort data från Skola24. Men det är stor skillnad på om en elev begär att ”ogiltig frånvaro från igår ska raderas”, ställt i förhållande till om en skola/kommun väljer att radera (gallra) data som inte längre kan anses vara aktuell.

Nova Softwares bedömning är att det utifrån Skollagen finns en laglig grund att spara data, men att stöd för gallring måste inkluderas i systemleveransen. Ett arbete bedrivs för närvarande för att se över möjligheter hur gallring kan förbättras (genom automatiserade inslag) i Skola24.

Exempel: för att kunna följa upp att elever får den utbildning (undervisningstid) de har rätt till (i enlighet med Skollagen), anses det nödvändigt att relaterad information också kan lagras (för att på så sätt underlätta skolans arbete, exempelvis med kontroll). Eftersom behandlingen innefattar personuppgifter, är bedömningen även att det är nödvändigt att Nova Software (i egenskap av personuppgiftsbiträde) kan radera (gallra) uppgifter enligt behov (instruktion).

Det ska också poängteras att skolan/kommunen (personuppgiftsansvarig) utgör den part som i sin tur mot Nova Software (personuppgiftsbiträdet) fattar beslut kring gallring. Dvs. det är inte Nova Software som på eget initiativ tar beslut kring gallring av data.

Med lagring avses generellt att en skola/kommun säger upp ett avtal med Nova Software, men där en bedömning görs att ”skolrelaterad data” måste lagras en viss tid. Ett lagringsavtal kan tecknas med Nova Software, vilket i sin tur reglerar hur länge data ska lagras.

2.12LAGRINGSPLATS (DATACENTER)

Nova Software lagrar i huvudsak data i ett eget datacenter placerat i Falköping. Åtkomst till detta utrymme är strikt begränsat till ett fåtal resurser. Utrymmet är vidare kopplat till avbrottsfri kraft (*UPS - Uninterruptible Power Supply*) samt utrustat med ett från övriga kontorsytor avskilt larm.

Vid arbete med backup (säkerhetskopior) finns två fysiska lagringsplatser. Ett brandsäkert utrymme i befintliga kontorsytor och ett brandsäkert utrymme på annan plats i Falköping. Syftet är undvika att lagring av media för säkerhetskopior förvaras på ett ställe – vilket kan vara förenat med en risk.

Ett undantag kring lagringsplats, är leveransen av Skola24 för en enskild kund, där underliggande avtal reglerar att data ska lagras på särskild plats med drift av en till Nova Software extern part.

För mer utförlig information om *skyddsåtgärder,* se även 3.1 Skyddsklassning.

3 Övrig information

Nedan presenteras övrig information som anses värdefull att redogöra.

3.1 SKYDDSKLASSNING

Nova Software genomför en s.k. *skyddsklassning* av de system som behandlar persondata. Ju högre skyddsklass, desto högre skyddsvärde – dvs. större behov av ”skyddsåtgärder” (eller förebyggande åtgärder). Revision av skyddsklass utförs löpande, där rådande skyddsklass också reglerar frekvens.

Skyddsklassningen kan ses som en anpassad tillämpning av det som inom GDPR omnämns som en DPIA (Data Protection Impact Assessement) – ”risk-/konsekvensbedömning”. Det är också utifrån GDPR en insats för att tillse att Nova Software vidtar *nödvändiga säkerhetsåtgärder för dataskydd*.

Exempel: ju högre skyddsklass, desto högre krav på åtgärder för att säkerställa hög tillgänglighet (så som redundans), åtgärder för att förhindra obehörig åtkomst (så som högre autentiseringsnivå), och åtgärder för att minimera dataförlust (så som hög frekvens av säkerhetskopiering och brandsäkerhetsskydd vid lagring av media.

Revision av skyddsklass innebär bl.a. att bedöma om lämplig skyddsklass råder, samt att utvärdera dess uppfyllnadsgrad, så som om definierade åtgärder för att förhindra obehörig åtkomst uppfylls.

Vid avvikelser, kan rapportering till en ansvarig roll (och/eller till en *ledningsfunktion*) initieras.

Skyddsklassningen för Skola24 medför bl.a. att systemet ska kunna levereras med stöd för 2faktor-autentisering (så som BankID), etablerade interna regelverk kring åtkomsthantering, monitorering samt att hög frekvens av backup tillämpas i kombination med krav på bl.a. brandsäkerhetsskydd.

Den skyddsklassning som utförs, utgår även från ett antal grundläggande faktorer, vilka oberoende av system som behandlar personuppgifter kan uttryckas som grundläggande skyddsåtgärder. När det kommer till *yttre skydd*, handlar det bl.a. om larm, passagessystem och avbrottsfri kraft (UPS). När det kommer till *inre skydd*, handlar det bl.a. om förebyggande funktioner för att förhindra angrepp av *skadlig programvara* (virus) och överbelastningsattacker (DDoS-attacker[4]).

3.2 DATASKYDDSPOLICY

Nova Software arbetar med att definiera innehåll i en Dataskyddspolicy. Denna policy kan enkelt beskrivet sägas innehålla en samling riktlinjer som löpande ska revideras med utgångspunkt från GDPR. Det kan vara allt från att se över rutiner kring gallring i Skola24, att säkerställa att riktlinjer för ”Privacy by design” tillämpas vid funktionella ändringar i Skola24, till att interna rutiner säkerställs, så som att gallring av persondata i Nova Softwares lönesystem utförs tillfredställande.

Exempel: ”Privacy by design” – att säkerställa *inbyggt integritet*. Det kan handla om att säkerställa att Skola24 i fall av tillförande av ny funktionalitet inte behandlar mer personuppgifter än vad som är nödvändigt för ändamålet, att ”fritextfält” undviks om möjligt, såväl som säkerställa att viss information enbart är åtkomlig för en given roll (dvs. inte publik).

3.3 DATASKYDDSGRUPP

Nova Software arbetar med etablering av en Dataskyddsgrupp, vilka med ledning av en DPO (Data

[4] DDoS – Distributed Denial of Service – attack för att förhindra normal användning av en tjänst en (”överbelastningsattack”).

Protection Officer - *Dataskyddsombud*) bl.a. ska arbeta med kontroller runt GDPR och dess efterlevnad, interna informations- och utbildningsinsatser, identifiering och stöd runt behov som rör GDPR (så som vid förändringsbehov i Skola24) samt att kunna bistå vid ”kundstöd”.

Tanken är att gruppen bemannas med kompetens inom bl.a. GDPR, teknik, avtal och skola.

För att nämna övriga exempel på arbetsuppgifter, kan det handla om att utföra skyddsklassning (ref. 3.1 Skyddsklassning), att arbeta med dataskyddspolicy (ref. 3.2 Dataskyddspolicy), samt att tillse att det finns information (*register*) över den behandling av personuppgifter som utförs på uppdrag av personuppgiftsansvariga (dvs. *för den personuppgiftsansvariges räkning*).

När det kommer till att föra *register,* så genomförs en utredning av olika system/leverantörer.

3.4 RAPPORTERING

I flera fall föreligger en rapporteringsskyldighet utifrån GDPR. I fall av exempelvis dataintrång så kan det vara nödvändigt att upprätta kontakt med Datainspektionen (tillsynsmyndighet). Det anses här viktigt att belysa att det är personuppgiftsansvarig som åläggs sådant ansvar. Det ansvar som ligger på Nova Software är att tillse att personuppgiftsansvarig informeras.

De utredningar som utförs inom detta område, syftar till att säkerställa att våran organisation vid övergången till GDPR är väl införstådda med vilka skyldigheter som är kopplade till Nova Software ifall av särskilda tillbud, såväl som att säkerställa att nödvändiga rutiner finns på plats. Vid genomför bl.a en genomlysning av processer runt- incident- och informationshantering.

3.5 NOVA EXCELLENCE

Vid bokning av kurser i Skola24 insamlas information om kostbehov. Syftet är att fånga eventuella behov som är nödvändiga att ta höjd för inför ett kurstillfälle som anordnas av Nova Software.

Det kan handla om allt från önskemål om vegankost till information om nötallergi. Denna typ av data kan klassificeras som känslig (ref 2.3 Personuppgifter och *känsliga personuppgifter*).

Vår bedömning är dock att det i föreliggande fall kan vara förenat med en viss risk att inte samla in denna typ av information. För att anknyta till rättslig grund (ref. 2.1 Rättslig grund) anses det även vara möjligt att motivera denna typ av personuppgiftsbehandling genom en intresseavvägning och hänvisning till ett berättigat intresse. Det anses slutligen nödvändigt att framföra att det utförs en utredning för att säkerställa rutiner för gallring när det kommer till *kursverksamhet*.

4 Nödvändiga kringsystem

För att initiera och underhålla den affärsrelation som uppstår vid avtalstecknande använder Nova Software två centrala kringsystem – Lime CRM (Lundalogik) och Visma (Visma).

Lime används bl.a. som ett kundregister (grundläggande information om Nova Softwares kunder), men även för arbete med offerter, avtal, kursverksamhet och support. Lime hanterar även underlag om fakturering utifrån avtal, vilket också överförs till Visma för att hantera kundfakturering.

För att anknyta till rättslig grund (ref. 2.2 Rättslig grund), anses den personuppgiftsbehandling som utförs bl.a. vara motiverad genom att det anses nödvändig för att fullgöra ett avtal (Punkt 2), men även genom en intresseavvägning och hänvisning till ett berättigat intresse (Punkt 3).

En utredning genomförs också för att se över om det kan vara nödvändigt att förtydliga ovan typ av systemstöd i kundavtal (för ändamål […] används systemstöd […]), eller om det i ett enklaste av läge kan räcka med att informera om denna typ av system via Nova Softwares externwebb.

Det anses slutligen viktigt att påvisa att övriga inslag som rör GDPR utreds kopplat till dessa system. Det handlar exempelvis om säkerställning av gallringsrutiner.

5 Versionshistorik

Versionshistorik			
[X.X]	[Datum]	Förnamn Efternamn	[Övergripande beskrivning av förändring]

Versionshistorik hanteras from v1.0 2017-12-06 >.