HÖGSKOLAN DALARNA

Undersökning av GDPR och NIS samt dess betydelse för enkla hemsidor

Författare: Tobias Wilhelmsson

Handledare: Hans Jones

Examinator: Mark Dougherty

Ämne/huvudsakliga studieområden: Datorteknik och juridik

Datum för examination: 2018-06-19

Dedikation

Till min fru Jenny och dotter Madicken för att ni finns där för mig och ger mig den kraft och energi som jag behöver.

Tack till

Jag vill tacka mina studiekamrater som har funnits där på resan genom studierna. Att ni har funnits där så att vi kunnat stötta och hjälpa varandra. Ni har varit mina klippor.

Tack till min handledare Hans Jones som har hjälpt mig att förstå och väglett mig till det slutliga arbetet jag sitter med idag. Tack för snabba och bra svar.

1. Abstrakt

I detta arbetet har det genomförts två undersökningar. Den ena undersökningen handlar om GDPR och den andra om NIS. Dessa två regelverk är skapade av EU för att säkra upp när det gäller cyberattacker och att styrka individers möjlighet att hantera sina personuppgifter. Det har även skapats en enkel hemsida i arbetet. Denna hemsidan är ett experiment för att ta reda på vad någon som äger eller tillhandahåller en enkel hemsida bör tänka på när det kommer till GDPR och NIS. Hemsidan i sig är tänkt att ge möjlighet för människor att träffa andra med samma intresse eller träffa de som befinner sig i liknande livssituationer. GDPR är en förnyelse av Sveriges tidigare lag PUL. GDPR är en förordning från EU vilket innebär att den måste följas mer noggrant än PUL. PUL var ett direktiv från EU. Ett direktiv väger inte lika tungt som en förordning. GDPR ger EU:s medlemsländers medborgare starkare rättigheter till deras personuppgifter. Det innebär att de har rätt att veta vad och varför personuppgifter hanteras. De har även rätt till radering vilket innebär att en organisation måste radera personuppgifter om de inte längre har någon anledning att fortsätta behandla dem. Det kan handla om rättslig påverkan eller en intresseavvägning om en personuppgift får behandlas vidare eller inte.
NIS är som sagt skapat av EU, detta är ett direktiv som beskrivit lite tidigare i detta stycke vad det innebär. Här har EU:S medlemsländer lite friare händer. Det finns mål som skall uppfyllas men medlemsländerna får själva bestämma hur målen skall uppnås. NIS handlar om cybersäkerheten inom EU. Det gäller att stärka den lägstanivå som finns. Jobba med att vara bättre förberedd om en incident skulle inträffa och på så sätt ge ett bättre grundskydd mot cyberattacker. Vad gäller en enkel hemsida så har GDPR en del att säga till om. Om man sparar data i en databas så skall de som personuppgifterna tillhör veta om det och samtycka till det. Det skall även kunna gå att få fram informationen som är sparad om personerna och även radering av personuppgifter om så önskas. En registrerad skall kunna få information om personuppgifter som sparas hos en personuppgiftsbehandlare utan att betala för det. När det gäller NIS och enkla hemsidor så är det i regel inget som rör den som tillhandahåller hemsidan eller hemsidans ägare. Det krävs i så fall att det är större företag med stor omsättning och som har huvudkontor i Sverige.

Nyckelord:

GDPR, NIS, hemsida, personuppgifter, personuppgiftsansvarig, säkerhet, HTML, PHP, Java-Script, CSS, EU

2 Innehåll

3. Terminologi

Förkortning/Begrepp	Förklaring
HTTPS	Hypertext Transfer Protocol Secure, göra en hemsidas data krypterad.
PHP	Hypertext Preprocessor, språk när man gör hemsidor.
GDPR	Dataskyddsförordningen, EU:s förordning angående behandling av personuppgifter.
NIS	Informationssäkerhet för samhällsviktiga och digitala tjänster.
HTML	HyperText Markup Language, ett sprk som används när man skapar hemsidor.
CSS	Cascading Style Sheets, används vid design av en hemsida.
JavaScript	Används vid skapandet av hemsidor.
PUL	Personuppgiftslagen, skydda personuppgifter. Byts ut mot GDPR.
EU	European Union.
ID	Ett nummer för att veta antalet.
CSIRT	Computer Security Incident Response Team.
IT	Informationsteknik.
MySQL	Ett språk för att hantera databaser.
Firebase	En tjänst från Google som skall underlätta vid hantering av hemsidor och applikationer.
Responsiv webbdesign	Anpassa hemsida för andra enheter som mobiltelefoner.
Databas	Ett sätt att spara data på.
Direktiv	EU sätter detta som en riktlinje
Förordning	EU sätter detta och väger tyngre än ett direktiv

4. Introduktion

4.1. Bakgrund

Arbetet inbegriper två undersökningar och en enkel konstruktion av en hemsida. Den ena undersökningen berör GDPR, en förordning som EU har skapat för att ge EU:s medborgare större rättigheter till sina personuppgifter. Den andra undersökningen handlar om NIS. NIS är ett direktiv från EU som är skapat för att förbereda och stärka cybersäkerheten inom EU:s medlemsländer. I detta arbetet kommer undersökningarna av GDPR och NIS att appliceras på den enkla hemsidan. Kommer en hemsida med inloggning att behöva hantera GDPR eller NIS? Vad behövs i så fall göras för att följa dessa regler. Utöver hemsidan så kommer det finnas en övergripande beskrivning av vad man behöver ta i beaktning när det gäller GDPR och NIS vid en konstruktion av en hemsida.

4.2. syfte

Detta arbetet har ett flertal olika syften. Det skall finnas en enkel och lättförståelig genomgång av GDPR och NIS. En fördjupning inom dessa områden. Syftet med hemsidan är att besökare skall kunna skapa ett konto och ta del av de tjänster som finns på sidan. Sedan har vi ett annat syfte där det handlar om att undersöka vad som gäller för detta projektets hemsida och andra hemsidor enligt GDPR och NIS. Om man tillhandahåller en hemsida, vad skall man då tänka på om man vill följa GDPR och NIS.

4.2.1. Mål

Målet med detta arbetet är att få en enkel överblick och förståelse om vad GDPR och NIS handlar om och vad som gäller om man har en hemsida med besökare. Vad man måste tänka på och vad man behöver ändra på. Vilka rättigheter har vi som äger våra personuppgifter och vilka skyldigheter har de som hanterar personuppgifter? Den enkla hemsidan skall fungera som tänkt och tjänsterna fungera som planerat. Målet är också att få en slags enkel förklaring om vad man behöver tänka på vid skapande eller ägande av en hemsida. Efter att man har läst detta arbetet skall man ha en lite bättre förståelse när det gäller GDPR och NIS. Även veta vad som gäller om man vill eller skall tillhandahålla en hemsida.

4.3. Metod

När det gäller undersökningen av GDPR och NIS så har detta arbetet använt sig av en kvalitativ metod. Det innebär att det skall vara en djupare förståelse av områdena som undersöks. Först har det samlats in information inom de olika undersökningsområdena och sedan har det sållats ut så att den mest anpassade informationen enligt arbetets menig sparats och undersökts.

Den andra delen har inneburit försök och tester. Testerna och försöken har lett arbetet framåt. Få fram de resultat som behövs för att hemsidan skall fungera som det är tänkt. Detta skulle kunna vara ett slags experiment.

4.4. Omfattning

När det gäller programmeringsspråk så kommer detta arbetet innefatta HTML, CSS, PHP och JavaScript. Arbetet kommer innehålla minst av JavaScript och inriktas mest på HTML och PHP. CSS kommer att användas så att hemsidan går att använda.

Detta arbetet har inte gått igenom allt inom GDPR och NIS. Det skulle vara alldeles för omfattande.

5. GDPR (**General Data Protection Regulation,** Dataskyddsförordningen, DSF)

Vi har nu följt personuppgiftslagen (PUL) för att skydda vår identitet från att spridas eller användas på ett negativt sätt. ”Europaparlamentets och rådets förordning om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter” (Datainspektionen 2016 s.1). EU medlemmar skall få en tryggare tillvaro när det handlar om hens personuppgifter. Genom att göra det till en förordning så säger EU att alla EU länder skall hålla samma standard. Detta minskar risken för kryphål som fanns inom PUL.

5.1. Vad är PUL (personuppgiftslagen)?

Det kan tyckas märkligt att PUL skall nämnas här. I själva verket är det lite av en självklarhet. PUL är baserad på ett direktiv från EU, ” Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter” (EUR-Lex 1995). PUL ersattes av GDPR den 25 maj 2018**.**

5.2. Vad är en förordning och ett direktiv från EU?

”En förordning är en bindande rättsakt som alla EU-länder ska tillämpa i sin helhet” (Europeiska Unionen, 2018). Det innebär att de länder som är med i EU måste anpassa sig till förordningen och inga undantag finns att hämta. ” Ett direktiv sätter upp vilka mål som medlemsländerna ska uppnå, men de får själva bestämma hur det ska gå till” (Europeiska Unionen, 2018). Detta innebär att en förordning väger betydligt tyngre än ett direktiv. GDPR är en förordning och tar plats istället för direktiv 95/46/EG som i Sverige blev PUL. Vid ett direktiv så har länderna mer fria händer hur de skall tackla frågan och själva göra upp en lag eller regel utifrån den informationen de fått från EU. En förordning är inte en tolkningsfråga utan det som står är det som gäller.

5.3. Vad är en personuppgift?

En personuppgift är en information som pekar mot en fysisk person. Är en IP-adress eller kakor en personuppgift enligt GDPR? Om endast en IP-adress är sparad och inte förknippad med någon annan handling som kan peka mot en fysisk person så är det inte en personuppgift. Likaså med kakor, om det inte är förknippat med en fysisk person så uppfyller det inte kravet för en personuppgift (Datainspektionen 2016 s.6). Om en hemsida som samlar in IP-adresser för att se antalet unika besökare och endast detta så är det ingen personuppgift. Om vi istället säger att vi vid en registrering vill samla in en IP-adress och på så sätt kan koppla ett namn till IP-adressen så blir det en personuppgift. En personuppgift är data som kan ledas till en fysisk person. Det finns system där man sätter ett ID på en användare. Ett ID i sig är ingen personuppgift men om ett ID går att länka till en person så blir även ett ID en personuppgift. Så man kan inte gömma sig bakom ett sådant system. En personuppgift är något som kan härleda till en fysisk person. Om vi sparar en plats i en databas är det ingen personuppgift men däremot om man sparar någons hemadress så kan det vara en personuppgift. Ett namn kan både vara och icke vara en personuppgift. Ett vanligt namn kopplat med ett vanligt efternamn behöver inte vara en personuppgift om det då inte är kopplat med något annat till den personen som en hemadress eller IP-adress.

Däremot kan ett ovanligt namn och ett ovanligt efternamn vara en personuppgift eftersom det kan direkt kopplas till en fysisk person.

5.4. Behandling av personuppgifter

Visa personuppgifter med respekt. Det är människors identitet som behandlas och bör behandlas med stort allvar. Vi har följt PUL till den 25 maj 2018 då GDPR tog plats istället för PUL. Behandlingen av personuppgifter kommer då att förtydligas och skärpas. PUL har gett oss bra direktiv och vägledning om hur vi skall bevara och ta hand om andras personuppgifter. Utvecklingen har gått snabbt framåt och våra personuppgifter är inte så pass personliga som EU vill längre. Därför har en förordning skapats från EU:s sida. Behandling av personuppgifter förtydligas ock skärps. Med PUL hade vi undantag såsom ostrukturerad text (SFS 2010:1969, personuppgiftslagen). I och med GDPR så kan vi inte hoppa över att behandla personuppgifter som finns inom exempelvis mail. En behandling av personuppgifter kan vara att man behöver skriva in namn och adress vid en eventuell registrering. Då måste personuppgiftsansvarige behandla hens personuppgifter exempelvis i en databas. All beröring av personuppgifter måste behandlas enligt GDPR. Ostrukturerad text skall även den behandlas med riktlinjer från GDPR. Personuppgifter skall behandlas på följande sätt. Endast de som är behöriga skall ha åtkomst. Vid en insamling av personuppgifter skall det framgå tydligt att personuppgifter samlas in. Det skall även samlas in på ett lagligt exempelvis via avtal. Det är inte godkänt att samla in personuppgifter som man inte behöver i stunden men kanske kan tänka sig att använda i framtiden. Endast nödvändiga personuppgifter och inga andra.

5.5. Straffet om man inte följer GDPR

Det finns ett bötesbelopp om man inte följer GDPR. Det kan bli en dyr historia om man medvetet väljer att inte följa GDPR. Om man motsätter sig GDPR så kan boten eller straffet bli ”administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4% av den totala globala årsomsättningen under föregående budgetår” (Europaparlamentets och rådets förordning (EU) 2016 artikel 83.6). Detta är maxbeloppet enligt GDPR. Detta belopp kommer endast krävas om den åtalade helt bortser från GDPR.

5.6. Rätt till radering

Detta kan låta överdrivet eller brutalt. Självklart är det inte en total radering av personen. Med andra ord kan man beskriva det som rätten att radera information från en organisation. en registrerad har rättighet att radera sina personuppgifter hos den personuppgiftsansvarige. Det får då inte vara en för lång väntetid innan detta blir gjort. För att den registrerade skall ha rätt till att få sina personuppgifter raderade så krävs något av följande. Att personuppgiften inte längre är behövande av personuppgiftsansvarige för att fullfölja tjänsterna som den registrerade vill använda. Om någon vill säga upp ett kontrakt eller säga upp sin registrering så skall även dennes personuppgifter raderas ut (Europaparlamentets och rådets förordning (EU) 2016 artikel 17.1). En registrerad har rätt att be om radering av personuppgifter vid specifika situationer. Den som är personuppgiftsansvarig måste då radera personuppgiften om inte skälet att behålla personuppgifterna väger tyngre än den registrerades önskan om att bli raderad (Europaparlamentets och rådets förordning (EU) 2016 artikel 21.1). Den registrerade har alltid rätt att anmärka om hens personuppgifter används vid marknadsföring (Europaparlamentets och rådets förordning (EU) 2016 artikel 21.2). visar det sig att den

registrerades personuppgifter har hanterats på ett olagligt sätt så har man rätt till radering (Europaparlamentets och rådets förordning (EU) 2016 artikel 17.1). Om något av kraven uppfylls av den registrerade så skall personuppgiftsansvarige radera personuppgifterna och radera länkar eller kopior som innehåller hens personuppgifter (Europaparlamentets och rådets förordning (EU) 2016 artikel 17.2). Rätt till radering gäller inte när yttrande- och informationsfrihet bedrivs eller inom myndighetsutövning. Raderingen kan bli utesluten om det handlar om folkhälsa så som förebyggande hälso- och sjukvård (Europaparlamentets och rådets förordning (EU) 2016 artikel 17.3). ” Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter” (Europaparlamentets och rådets förordning (EU) 2016 artikel 89).

5.7. Vilka personuppgifter får man inte behandla?

Det finns vissa personuppgifter som inte är tillåtna att behandlas av en personuppgiftsansvarig. Här nedan kommer en lista på dessa personuppgifter.

- Ras och etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska uppgifter eller biometriska uppgifter för att identifiera fysisk person
- Hälsa, sexualliv eller sexuell läggning

(Europaparlamentets och rådets förordning (EU) 2016 artikel 9.1).

5.8. Samtycke vid behandling av barns personuppgifter

Här finns det speciella regler som är anpassade för just barnen inom EU. I grunden av GDPR så gäller målsmans underskrift på något sätt när barnet är yngre än 16 år. Är barnet 16 år eller äldre så kan hen registrera sig på en sida med sina personuppgifter utan målsmans underskrift. Om den som vill registrera sig är yngre än 16 år så skall den som har ansvar för personuppgifterna samla in underskrift av målsman till det registrerade barnet. Denna insamling sker med tillgänglig teknik. Kanske kan det vara att målsman skannar in en underskrift på ett papper som personuppgiftsansvarig fixat åt dem i ett mail. Åldersgränsen har en möjlig variation. Som sagt så är grunden i GDPR 16 år men det finns möjlighet för en medlemsstat att ändra den till en lägre, dock inte lägre än 13 år (Europaparlamentets och rådets förordning (EU) 2016 artikel 8).

5.9. Personuppgiftsansvarig

Vem kan få personuppgiftsansvarig som titel? En förening, ett aktiebolag, stiftelse eller myndighet som behandlar personuppgiften är persongiftsansvarig. Ingen VD eller någon annan som är anställd vi organisationen kan då vara personuppgiftsansvarig. Däremot finns det undantag där det kan vara en person som är personuppgiftsansvarig. Om en person har startat något som heter enskild firma eller enskild näringsverksamhet så blir då personen i fråga personuppgiftsansvarig (Datainspektionen 2017). Detta innebär att det den som står under enskild firma själv betalar skuld och att avtal går rätt till och inte bryts. Ägaren är då innehavare (Bolagsverket 2014). Den personuppgiftsansvarige har som ansvar att se till så

att personuppgifter behandlas korrekt och inom ramarna för GDPR. Personuppgiftsansvarige har möjlighet att överlämna uppgiften att behandla personuppgifter. Däremot går det inte att lämna bort ansvaret för de personuppgifter som den personuppgiftsansvarige behandlar. Är man personuppgiftsansvarig som ovan exempelvis ett aktiebolag så är det aktiebolaget som är personuppgiftsansvarig och det förblir de så länge det finns personuppgifter att behandla inom aktiebolaget. (Datainspektionen 2017-06-29)

5.10. Personuppgiftsbiträde

Detta är inte någon person inom den personuppgiftsansvariges organisation. Det är någon eller en organisation utanför personuppgiftsansvariges organisation. Personuppgiftsbiträde kan vara en fysisk eller juridisk person. Den personuppgiftsansvarige kan ta hjälp utifrån sin egna organisation för att få fram en produkt eller resultat som behövs inom personuppgiftsansvariges organisation. Då någon utanför personuppgiftsansvariges organisation behandlar personuppgiften så blir denne ett personuppgiftsbiträde till den som gett organisationen uppgiften att behandla personuppgiften. Kravet hos personuppgiftsbiträdet är att de skall behandla personuppgiften enligt GDPR. Personuppgiftsbiträdet måste garantera att personuppgifterna skyddas på korrekt sätt. Det kommer att ske en överenskommelse mellan personuppgiftsansvarige och personuppgiftbiträdet vad som får och inte får göras med personuppgifterna. Personuppgiftbiträde får i sin tur anlita ett biträde men endast om personuppgiftsansvarige godkänner till detta. Alltså får de inte anlita ett eget biträde för de personuppgifter som kommer från någon annan personuppgiftsansvarig om inte det är överenskommet. Biträdet har ansvar för att ha en passande nivå av säkerhet för personuppgifterna och dokumentera behandlingen av personuppgifterna (Datainspektionen 2017-09-28).

5.11. Dataskyddsombud

Dataskyddsombud är en fysisk person med goda kunskaper inom GDPR. Deras uppgift är att få personuppgiftsansvarige eller personuppgiftsbiträdet att följa GDPR eller att få organisationens mål att följa GDPR. Dataskyddsombud skall ha omtanke vid behandling av personuppgifter (Datainspektionen 2016 s.56 artikel 39).

5.12. Samtycke

En användare skall ha möjlighet att välja samtycke på ett smidigt, enkelt och tydligt sätt. Användaren skall självmant intyga att hens personuppgifter behandlas hos den personuppgiftsansvarige. Denna handling får icke ske automatiskt utan det är användaren själv som måste godta att behandlingen av personuppgifter får ske hos den personuppgiftsansvarige. Det innebär att ingen ruta som samtycker behandling får vara ikryssad automatiskt utan endast av användaren själv. Sätt som kan användas för samtycke kan vara att kryssa i en ruta, en skriftlig bekännelse eller muntligt erkännande. Det skall vara en klar beskrivning om att användaren lämnar ett godkännande och att hens personuppgifter kommer att behandlas av den personuppgiftsansvarige (Datainspektionen 2016 s.6 stycke 32). Den som är personuppgiftsansvarig bör kunna förklara eller visa att samtycke har skett vid exempelvis en registrering. Användaren borde ha fått veta hur lång tid som personuppgifterna kommer att behandlas hos den personuppgiftsansvarige. Samtycket måste vara tydligt och skrivet på ett enkelt språk. Användaren skall inte behöva leta efter några viktiga detaljer. Det skall vara enkelt att läsa och förstå vad man samtycker till. Detta betyder att man inte kan gömma ett samtycke i en lång text eller med mindre

bokstäver. Man får inte göra det svårt för användaren att förstå samtycket. Avsikten med behandlingen av personuppgifter bör vara enkla att förstå av användaren. Användaren bör ha en identitet på den personuppgiftsbehandlare som kommer att behandla hens personuppgifter. Om personuppgiftsansvarig kommer att anlita ett biträde så skall detta också tydligt stå vid ett samtycke av en registrering. Samtycket kommer också att förflyttas till personuppgiftbiträdet (Datainspektionen 2016 s.8 stycke 42).

5.13. Missöde med personuppgifter

Vid händelse då det finns en risk att personuppgifter kan ha kommit till fel händer eller att de finns något tecken på att något hänt personuppgifter hos personuppgiftsansvarige så skall detta anmälas till tillsynsmyndigheten inom 72 timmar när man upptäck missödet gällande behandlingen av personuppgifter. Om en sådan här händelse inte rättas till tillräckligt snabbt så kan den fysiska personen ta skada av händelsen. Olika scenarion som kan drabba den registrerade användaren kan vara att förlora hanteringen av sina personuppgifter, diskriminering, identitetsstöld eller bedrägeri. De som har personuppgifter som behandlas hos personuppgiftsansvarig bör så snabbt som möjligt kontaktas om läget om det visar sig vara ett allvarligt missöde och den fysiska personen kan ha en risk att personuppgifterna hamnar på villovägar och att detta kan skada den registrerades frihet eller rättigheter. Det borde också framgå vad som hänt vid det specifika missödet. Personuppgiftsansvarige skall se till att rätt säkerhetsåtgärd görs. Detta skall ske i nära samarbete med tillsynsmyndigheten eller med brottsbekämpande myndigheter om de behöver kallas in (Datainspektionen 2016 s.16–17 stycke 85–86).

5.14. Få ut sin information

En registrerad har rätt att få ut information om personuppgifter som angår den registrerade i fråga från personuppgiftsansvarig vid begäran. En registrerad har inte bara rätt att få information om de behandlande uppgifterna utsatts av ett dataintrång utan de har själva rätt att kräva informationen utan att någon speciell situation har uppstått. Detta skall ske enkelt och med den teknik som finns tillgänglig. Det får inte tillkomma några kostnader för att få ut sin information. Det är en rättighet som är kostnadsfri och det skall komma med en tydlig och lättläst text så att den registrerade enkelt kan förstå vilka uppgifter som behandlas om hen. Denna funktion gör det enklare för användaren att se så all information stämmer. Om personuppgiften inte är korrekt så skall detta ändras (Datainspektionen 2017-04-19).

6. NIS-direktivet (nätverks- och informationssystem direktivet)

Den 10 maj 2018 kommer säkerheten inom nätverk- och informationssystem att skärpas inom EU. Detta kommer att gälla leverantörer av digitala tjänster och samhällsviktiga tjänster.Det måste finnas en bättre tillsyn, det skall rapporteras vid incidenter och det skall finnas säkerhetsåtgärden (Myndigheten för samhällsskydd och beredskap). ”Om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela Unionen” (Statens offentliga utredningar SOU:2017:36, Bilaga 2 s.1). NIS-direktivet är ett direktiv från EU, vilket innebär att medlemsländerna skall ta till sig direktivet till sina lagar och regler. Ett direktiv är mer fritt än en förordning som GDPR är. Men det innebär inte att man kan hoppa över ett direktiv. Det skall följas på sitt sätt. NIS är den första lagstiftningen som EU gör där det handlar om en ökad cybersäkerhet. EU vill att alla medlemsländer skall hålla en jämnare och högre nivå när det gäller cybersäkerhet inom EU:s medlemsländer.

6.1. Varför behövs NIS?

Idag så ser vi att tjänster och system inom nätverk och information har en stor betydelse i vår värld. För att vi skall kunna använda dessa tekniker så behöver vi en starkare säkerhet. Det är så otroligt mycket som står på spel för att inte ha en ökad cybersäkerhet. Incidenter eller intrång av nätverk och informationssystem kommer att vara mer betydande och oftare förekommande. Detta skapa en fara mot nätverks- och informationssystemens funktion. Ett sådant angrepp kan göra en stor skada i samhället. Detta kan medföra driftavbrott eller ekonomisk skada. Överföring av tjänster och produkter via internet är en stor del i samhället idag. Avbrott av detta kan göra stor skada på länder inom EU. En stabil cybersäkerhet är således viktigt att ha med i beräkningarna. En grupp borde skapas där representanter från EU:s medlemsländer samlas som skall främja samarbetet mellan EU:s medlemsländer angående nätverks- och informationssystemen. Det krävs då att varje medlemsland har en minimikapacitet som garanterar en högklassig säkerhetsnivå inom nätverks- och informationssystemen. (Statens offentliga utredningar SOU:2017:36, Bilaga 2 s.1-2 stycke 1-4)

6.2. NIS-direktivet ger medlemsländerna skyldigheter

EU vill ha en högre och säkrare nivå på sina medlemsländer. Detta för att öka tryggheten av den inre marknaden. Det som NIS-direktivet vill att medlemsländerna tar sig an är följande.

- ”anta en nationell strategi för säkerhet i nätverk och informationssystem (artikel 7),
- införa säkerhets- och incidentrapporteringskrav för leverantörer av samhällsviktiga tjänster och för leverantörer av digitala tjänster (artiklarna 14.1–3 och 16.1–3),
- utse nationella behöriga myndigheter, nationella kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (CSIRTenheter) och reglera samarbetet dem emellan (artiklarna 8.1, 8.3, 9.1 och 10),
- ingå i en samarbetsgrupp för strategiskt samarbete och informationsutbyte (artikel 11) och
- ingå i ett nätverk för enheter för hantering av it-säkerhetsincidenter

(CSIRT-nätverk) (artikel 12).

Medlemsstaterna ska också, senast den 9 november 2018,

- identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium, och i det syftet
- upprätta en förteckning över tjänster som är viktiga för att upprätthålla kritisk samhällelig och/eller ekonomisk verksamhet (artikel 5.1, 5.3 och 5.2 a) ’2(Statens offentliga utredningar SOU:2017:36, s.49).

6.3. Sveriges Tillsynsmyndigheter

Det finns indelningar av tillsynsmyndigheter. Dessa tillsynsmyndigheter skall ha olika indelningar inom tillsyn. Det innebär att de skall ha koll på vad som händer inom deras områden och föra vidare information om någon incident framkommer. Det finns fler tillsynsmyndigheter än vad som tas upp i detta stycket, men här namnges några få av dem. Digital infrastruktur och digitala tjänster är Post- och telestyrelsen tillsynsmyndighet för. Energi är Statens energimyndighet tillsynsmyndighet för och Livsmedelsverket är tillsynsmyndighet för leverans och fördelning av dricksvatten. (Statens offentliga utredningar SOU:2017:36, s.167 kapitel 8.5.2). Dessa områden skulle kunna ta stor skada vid en eventuell incident.

6.4. Digitala tjänster

En digital tjänst kan vara en plats på internet där konsumenter eller näringsidkare kan ingå i internetbaserade köpeavtal eller tjänsteavtal med näringsidkare. Med detta innebär det att om man har en hemsida som säljer saker eller tjänster så ingår man inom digitala tjänster. En tjänst som ger besökaren en möjlighet till sökning ut på internet med hjälp av nyckelord, en fras eller andra sätt som ger träffar via sökmotorn. En molntjänst kan också vara en digital tjänst.

Det som är viktigt att tillägga och veta om är att de beskrivna områdena inom digitala tjänster går under NIS i Sverige om följande krav kan uppfyllas. Om huvudkontoret befinner sig i Sverige, en årsomsättning på 10 000 000 EUR, för att vara en digital tjänst inom NIS så skall organisationen ha mer än 50 anställda och inte vara hårdvaru- eller mjukvarutillverkare. Detta innebär att om man har tjänster som liknar de beskrivna i första stycket och har en organisation som följer kraven i andra stycket så är det är digital tjänst inom NIS.

6.5. Sanktioner

Det finns ett förslag till sanktioner till dem som inte följer NIS och har tjänster som faktiskt lyder under NIS. Vissa av dessa är omnämnda i stycket Sveriges Tillsynsmyndigheter. (Statens offentliga utredningar SOU:2017:36, s.190 kapitel 9.6.4) Det förslag som ligger inom NIS-direktivet är en avgift från 5 000 kronor upp till 10 EUR kronor om man inte väljer att följa NIS. Det kan vara antingen ett bestämt belopp eller förenad med verksamhetens årsomsättning. Det skall vara ett så betydande belopp att man hellre vill följa NIS än att ta avgiften.

6.6. Krav och rapportering

(Statens offentliga utredningar SOU:2017:36, s.18-19) Kravet som gäller för de som hanterar tjänster som digitala tjänster och samhällsviktiga tjänster är att de tekniska och organisatoriska insatser när det kommer till att behandla risker i deras nätverk och informationssystem skall vara lämpligt för sitt ändamål. Om ett intrång har skett så skall de ha gjort ett förarbete som gör att incidenten eller intrånget inte tar lika stor skada som det skulle kunna ha gjort om inte förberedelserna hade gjorts. De som är leverantörer skall ta möjliga risker i beaktning och arbeta för att minska att dessa företeelser kommer att ske. Om en incident har varit fram så skall de som blivit drabbade kontakta CSRIT-enheten. Detta måste ske utan onödig försening och om incidenten är avsevärd när det gäller digitala tjänster eller om samhällsviktiga tjänsters incidenter är betydande.

6.7. CSIRT (Computer Security Incident Response Team)

CSIRT är ett incidenthanteringsorgan, där man skall diskutera IT-incidenter mellan EU:s medlemsländer. I Sverige är myndigheten för samhällsskydd och beredskap (MSB) som axlar rollen som CSIRT. Om en incident gällande IT sker så skall detta meddelas till MSB. De incidenter som sker inom de olika tillsynsmyndigheter som det skrivits om tidigare i detta arbetet bör också hamna hos CSIRT alltså MSB för att kunna få en helhetsbild så att NIS kan följas så bra som möjligt. De olika ansvarsområdena stannar fortfarande hos den utvalda tillsynsmyndighet men för att få en helhet i vad som händer så bör informationen samlas på ett ställe för att det skall bli enklare att utreda en helhetsbild (Statens offentliga utredningar SOU:2017:36, bilaga 1, s.310-312)

6.8. Nationell strategi

Regeringen tar denna fråga seriöst och vill främja den nationella strategin. Regeringen skall så gott de kan anpassa sig så att den nationella strategin efterliknar NIS så mycket som möjligt (Statens offentliga utredningar SOU:2017:36, s.50, kapitel 3.2.1). Den nationella strategi är till för att bevara en hög standard när det gäller säkerheten inom nätverks- och informationssystem. Den nationella strategi skall utföra de strategiska målsättningarna och hantera de politiska åtgärder som skall verkställas (Statens offentliga utredningar SOU:2017:36, bilaga 2, s.5).

6.9. Säkerhetsåtgärder och riskhantering

NIS-direktivet kommer med en plan att de som hanterar samhällsviktiga tjänster skall använda sig av en lämplig och avvägd teknisk och organisatorisk handling för att förebygga hot inom nätverk- och informationssystemen som tillhandahålls inom dennes sysselsättning. Hoten som ställs mot organisationens sysselsättning skall vara tillräckligt säker för att användas. De som hanterar samhällsviktiga tjänster skall avvärja kommande hot så gott de

kan och göra risken för en incident så liten som möjligt. De som hanterar samhällsviktiga tjänster skall också skapa en årlig uppdaterad riskanalys där det finns ett förslag för hantering om en incident skulle bli verklig. De skall också hjälpa de olika tillsynsmyndigheterna. Leverantören av samhällsviktiga tjänster skall ha hänsynstagande på den senaste utvecklingen av teknik och hålla en nivå på säkerheten inom nätverk- och informationssystemen som är anpassad för det möjliga hotet. Det skall också finnas ett arbete som förebygger och hittar hoten för att minska på incidenter. Nationella strategin som skapats skall ha en insikt i denna riskbedömningsplan (Statens offentliga utredningar SOU:2017:36, s.128-130).

6.10. säkerhetsanalys

Inom organisationen skall en säkerhetsanalys finnas. Den skall bland annat innehålla en beskrivning om information som ska vara hemlig för att det kan vara en säkerhetsrisk för riket. Det skall också stå beskrivet vilka konstruktioner som skall ha ett säkerhetsskydd för att styrka rikets säkerhet (Statens offentliga utredningar SOU:2017:36, s.84). Avvägningar för att få fram de bästa skyddsåtgärder skall också hanteras inom en säkerhetsanalys (Statens offentliga utredningar SOU:2017:36, s.96). ” Resultatet av undersökningen (säkerhetsanalys) ska dokumenteras” (Statens offentliga utredningar SOU:2017:36, s.111). För att kunna få fram det bästa skyddsåtgärderna så bör man veta om vilka hot som kan uppstå. Göra ett skriftlig arbete om vilka hot som kan komma att bli verklighet. Det finns flertalet olika hot mot organisationer idag så här kan man gräva ner sig ordentligt. För att kunna fullfölja en säkerhetsanalys som vill få fram det bästa skyddsåtgärderna så behöver man veta vilka hot som finns. De hot man inte förbereder sig för kan man inte heller skydda sig emot.

7. Skapandet av hemsidan

Under detta kapitel kommer det att göras en lite mer detaljerad genomgång av hemsidan, dess konstruktion, tjänster och skapandet. Här kommer det också att vara en koppling till GDPR och NIS. Vad behöver man tänka på och hur skall man gå till väga för att följa dessa regler som EU satt.

7.1. Hemsidans syfte

Syftet med den enkla hemsidan är att besökare skall kunna skapa ett konto. Med hjälp av det kontot skall de kunna placera sig i en kö. Kön består av att man säger stad och intresse/livssituation man befinner sig i. När det är tio personer med samma kö-inställningar så skickas ett mail till förslagsvis en restaurang. Restaurangen får frågan om det finns plats för besöket. Tanken bakom hela hemsidan är att folk som har samma intresse eller befinner sig i liknande livssituationer skall kunna mötas och lära känna varandra.

7.2. Målgrupp

När det gäller målgrupp måste man ta hänsyn till GDPR. GDPR säger att man får registrera sig på en hemsida utan målsmans underskrift när man är 16 år eller äldre. För att undvika hanterandet av målsmans underskrift så skall man vara 16 år eller äldre för att få ta del av hemsidans tjänster. Målgruppen för projektet är personer som är 16 år eller äldre och som söker nya bekantskaper. Intressen och livssituation är en metod för att underlätta sökandet.

7.3. Hemsidan

Hemsidan skall vara ett forum där folk skall kunna ha en möjlighet att träffa nya människor. Tanken är att det hemsidan ska vara lättnavigerad. Både ung som gammal skall kunna besöka hemsidan och förstå direkt vad det handlar om och vilka tjänster som finns att använda sig av. Hemsidan skall vara en säker plats för besökare och användare. De som registrerar sig eller besöker hemsidan skall kunna känna sig trygga. Vilken enhet som än besöker hemsidan skall kunna visa och använda innehållet oavsett vilken storlek på skärmen enheten än har.

7.4. Design

Vid skapandet av hemsidan och dess design så används HTML, CSS och JavaScript för att göra en hemsida som tydligt beskriver de funktioner som finns att tillhandahålla. Detta kan tyckas vara en svår uppgift eftersom att smak och tycke är olika för varje individ som besöker hemsidan. Det är enkelt att lägga ner för mycket tid på design och utseende på en hemsida. Det gäller att man kommer till en punkt där designen uppfyller skaparens intresse. Utseendet får växa fram allt eftersom arbetet fortgår. Det kommer nya funktioner och tjänster till hemsidan som kan få konsekvenser på designen. Därför är det ett tips att låta denna delen vänta tills det närmar sig slutresultatet. Denna hemsidan har fått en design som

inte fyller hela skärmen för besökaren utan centrerar innehållet och låter fokuset vara koncentrerat mot mitten.

Figur 2 En bild på hemsidan just nu. Ej helt klar men i alla fall en förståelse av designen.

Tydliga länkar och en första bild som tydligt säger ”klicka här för att veta mer!”. Finns självklart saker att jobba på men en grund att stå på.

7.5. Funktion

Tanken är att en användare skall kunna skapa ett konto. När användaren väl är inloggad skall hen kunna välja på olika ämnen, exempelvis ny i stan, film eller sport. Sedan skall hen klicka i vilken stad det gäller. Alla dessa val är förprogrammerade så att användaren har bara ett visst antal valmöjligheter. När dessa val är ikryssade så kommer användarens namn att placeras i en väntelista. När denna lista har uppnått tio personer så kommer ett mail skickas till exempelvis en restaurang. Restaurangen svarar om det finns plats den specifika kvällen. Sedan skickas ett mail till alla i den kön om tid och plats. De svarar på mailet och är det tillräckligt många som tackar ja blir träffen av. Här behöver projektet ta del av reglerna i GDPR (se avsnitt 5.4). När någon registrerar sig på sidan kommer det att visas en ruta. För att komma vidare till att registrera sig måste besökaren godkänna att personuppgifter kommer att hanteras och att besökaren är minst 16 år gammal. Först då kan besökaren registrera ett konto. Detta på grund av GDPR och dess regler.

7.6. Responsiv webbdesign

”Responsiv webbdesign (engelska Responsive Web Design, RWD) innebär webbdesign som tillåter layouten att förändras beroende på vilken skärmstorlek och skärmupplösning som besökaren har” (Wikipedia responsiv). Denna teknik innebär att vilken enhet man än besöker en hemsida med kan få med allt innehåll. Det är en skillnad på att besöka en hemsida med en dator eller en mobil. Bildskärmarna är det olika upplösning och olika storlekar på. En

mobil som har en mindre skärm än en dator visar upp en hemsida i en mindre skala. Detta måste man ta med i beräkningen och ändra hemsidan så att den blir responsiv.

7.7. Databas

Databasen är en otroligt viktig del av att skapa en hemsida om man tänkt hantera data från besökare. Självklart behöver man inte en databas för att få en hemsida att fungera. För att hemsidan som skapas i detta arbete skall fungera så måste det finnas en databas som hanterar information från de olika användarna som är registrerade på hemsidan. Detta projekt kommer att använda sig av en databas för att hantera användare och de tjänster som hemsidan tillhandahåller. I början fanns en fundering på två olika databaser som skulle användas i detta projekt. Den ena är MySQL och den andra är Firebase. MySQL är ett språk som man får koda själv och göra de inställningar som krävs. Detta kan vara tidskrävande och problematiskt i vissa stunder. Firebase är en molntjänst från Google. Det startade 2011 och har växt sedan dess. De är en tjänst med flera funktioner. I detta arbetet så har funktionen att logga in undersökts närmre. Det verkar vara ett smidigt sätt att koppla sin hemsida till för att skapa användare. En funktion som också är bra är att man enkelt kan fråga om användaren vill logga in med ett annat konto så som Google konto. I detta arbetet har inriktningen varit att använda MySQL. Detta gör att hemsidans ägare har mer koll på uppgifterna och kan själv hantera hur data skall sparas i en databas. Databasen som detta projektet hanterar kommer att ta del av GDPR och dess regler. Bara de som har nytta av att komma åt databasen skall ha befogenhet till databasen.

7.7.1. Vilka personuppgifter kommer sparas i databasen

Som beskrivet i GDPR tidigare så är en personuppgift en information som pekar på en fysisk person (se 5.3.). I detta projekt kommer det inte vara så många personuppgifter som behandlas. Egentligen är det bara en personuppgift som inte alltid är en personuppgift nämligen användarnas mail. En mail kan vara så specifik att det kan leda till en fysisk person så därför bör den hanteras som en personuppgift.

7.7.2. Viktigt att tänka på när man behandlar data i en databas

Det är viktigt att tänka igenom vad som kan vara en personuppgift i databasen. En personuppgift är en information som kan leda till en fysisk person. Det kan vara namn, bostad och mer därtill. Man bör veta vad i databasen om är en personuppgift.

7.8. Säkerhet

Vad innebär säkerhet när det kommer till hemsidor och databaser? Detta ämne/område är väldigt omfattande och det skulle ta lång tid att gå igenom allt. Det finns små som stora säkerhetstekniker att använda sig av på sin hemsida. En av de större är HTTPS Hypertext Transfer Protocol Secure), ett protokoll för krypterad transport av data (Wikipedia HTTPS). Vad är det som är så bra med HTTPS kan man fråga sig. Det handlar om att skydda sina

användare och besökare. Skillnaden mellan HTTP och HTTPS är just S som står för secure. När en hemsida är säker så krypteras all data som flyttas till och ifrån hemsidan. Detta gör att utomstående inte kan se vad som händer.

Det finns en hel del teknik som gör att man kan skapa en säker databas. En viktig del är att göra backup regelbundet. Om någon skulle lyckas få åtkomst av databasen gäller det att snabbt kunna återställa databasen till senaste fungerande period. Har man ingen backup så blir det svårt att veta vad som har förändrats efter ett ingrepp av exempelvis en hacker. Den som hanterar databasen kan se till att ha en databas som ändras när användaren gör sina inställningar eller använder tjänsterna. Då kan hen som hanterar databasen gå igenom det som ändrats och se om det är tillförlitliga data och sedan själv ändra den databasen som är synkroniserad med hemsidan. Som det ser ut nu kommer det göras backupper på databasen manuellt vilket innebär att ägaren till hemsidan antingen gör detta själv eller ta hjälp av någon. Hur ofta det skall ske är upp till ägaren at avgöra. I detta projektet så är tanken att två eller fler backuper i veckan skall göras.

7.9. Besökare

Tanken är att ha koll på antalet besök som hemsidan får per dag eller vid en speciell tidpunkt på ett dygn. Det skall även finnas en räknare som räknar antalet unika IP-adresser som besöker hemsidan. Denna information behövs för att veta intresset av hemsidan hos besökarna. Antalet unika IP-adresser berättar antalet olika enheter som varit i kontakt med hemsidan. Den informationen är viktig för att veta om det tillkommer nya besökare eller om det är ett visst antal besökare som återkommer till hemsidan. Databasen hanterar antalet besökare vid en viss tidpunkt. Varje gång förstasidan laddas upp på en enhet så ökar antalet med plus ett. Det loggas också i databasen vilken tid användaren besökte förstasidan. Denna funktion är bra att ha för att få information när på dygnet det är som mest trafik på hemsidan. I framtiden kanske det kommer att finnas olika erbjudanden för gamla som nya användare. Då kan det vara bra att veta under vilka perioder som det är flest besökare och på så sätt se vilka erbjudande som lockar flest användare. IP-adressen sparas i en databas och på så sätt kan man säga åt databasen att endast spara unika IP-adresser. Då kan man enkelt se hur många unika besökare hemsidan haft på hemsidan. Det finns redan företag som hanterar dessa funktioner och mer därtill. I examensarbetets hemsida har Hypertext processor använts. Anledningen till att göra en enkel räknare med hjälp av Hypertext Preprocessor (PHP) är att själv ha informationen enkelt och lättåtkomligt. Inte bara förlita sig helt på andra företag utan själv ha sina egna uppgifter så gott det bara går. Detta projektet kommer säkert använda sig av andra företags tjänster till en viss del i slutändan. Det kan visa sig att projektet till slut endast använder sig av andra företags tjänster. Det är en trygghet i att ha kvar funktionen och informationen på hemsidan. Det kan hända att företaget slutar med dessa funktioner eller kommer att börja ta ut en summa för deras arbete. Finns det redan en enkel räknare så har man fortfarande den informationen även om andra företag skulle sluta med sina tjänster. Vad gäller GDPR inom detta stycke så handlar det om att hantera IP-adresser. En IP-adress kan man behandla så länge det inte pekar mot en fysisk person. Reglerna inom GDPR säger att en IP-adress inte är en personuppgift så länge det inte finns annan information knutet till IP-adressen som kan leda till en fysisk person. I projektets fall så är det endast en IP-adress som sparas på så sätt är IP-adressen ingen personuppgift enligt GDPR.

7.10. Användarnas rättigheter

Användarna kommer genom GDPR få mer rättigheter på sin sida. Det gäller bland annat rätten till radering. Om en personuppgiftsansvarig inte längre behöver behandla en användares personuppgifter så måste personuppgiftsansvarige radera dessa personuppgifter från databasen. Vid en eventuell avregistrering så borde personuppgifterna raderas i samband med avregistreringen. En användare har rätt att veta vilka personuppgifter som behandlas hos den personuppgiftsansvarige. Det innebär att man vid en förfrågan av en användare måste visa vilka av hens personuppgifter som behandlas i databasen eller inom andra områden så som mail. Detta måste ske utan någon kostnad för användaren. En viktig detalj inom GDPR är att vara tydlig från första början. Vid en registrering måste tydligt framgå vilka personuppgifter som kommer att behandlas. Det måste också framgå varför man måste behandla dessa personuppgifter. GDPR har en tydlig regel om ålder när det gäller behandling av personuppgifter. I Sverige gäller målsmans underskrift för de personer som är under 16 år. Detta projektet kommer att använda sig av en kryssfunktion vid en eventuell registrering. Kryssar man i denna ruta så ger man ett medgivande att man befinner sig i rätt ålder för att registrera sig utan målsmans underskrift. Det måste också stå tydligt hur länge en personuppgift behandlas hos den personuppgiftsansvarige. Vid denna information så måste man låta användaren lämna ett tydligt och enkelt samtycke på att de tillåter att man behandlar deras personuppgifter i sin databas. Detta kommer att likna kryssrutan för medgivande av ålder.

7.11. Andra detaljer med DPR som är bra att tänka på

Behövs ett personuppgiftsbiträde (se 5.10). Kommer personuppgifter att behandlas av tredje part alltså en utomstående organisation? Behövs ett dataskyddsombud kopplat till organisationen för att kolla så att GDPR följs?

7.12. Vad behöver man tänka på när det gäller NIS?

För arbetets lilla projekt med att skapa en hemsida och för de flesta hemsidor generellt så finns ingen koppling till NIS. NIS är flera nivåer över detta arbetets projekt och på så sätt så behöver man inte anpassa något inom NIS. Flera nivåer högre i detta fallet menas att det handlar om myndigheter och etablerade företag. För att vara en digital tjänst så kan man tillhandahålla en sälj- och köptjänst via sin hemsida, hemsidan kan också vara en sökmotor som söker över hela internet eller hantera en molntjänst. Så visst kan en hemsida innefatta dessa tjänster men det finns krav för att behöva följa NIS i Sverige (se avsnitt 6.4 för mer information). När det gäller infrastruktur, vatten och dess transport så handlar det om tillsynsmyndigheter vilket en vanlig hemsida i regel inte har att göra med. På så sätt så har är NIS något utöver en grundlig hemsida.

8. Resultat

Detta arbetet har haft två undersökningar inom områdena GDPR och NIS. Det har även ingått att skapa en enkel hemsida och genom den ta reda på vad som behöver tas i beaktning när det gäller GDPR och NIS. GDPR och NIS är två olika restriktioner från EU. GDPR är en förordning medan NIS är ett direktiv. Förordning är en tyngre restriktion än ett direktiv. Detta innebär att förordning skall följas till punkt och pricka. Det finns vissa undantag där EU:s nationer själva får bestämma så som ålder för att behöva målsmans underskrift. I grunden av GDPR är det 16 år och äldre som inte behöver målsmans underskrift. Denna ålder kan medlemsländerna reglera en aning, den lägsta åldern utan att behöva ha målsmans underskrift är 13 år. Förutom undantagen så måste en förordning följas. Ett direktiv är olika mål som EU:s medlemsländer själva skall uppfylla på deras sätt.
GDPR är menat att vara ett skydd till EU:s länders medborgare. Det handlar om att de har större rättigheter och mer makt att kunna hantera och att ta till vara sina personuppgifter. En personuppgift är en information som kan härleda till en fysisk person. Vad har vi då fått för nya och starkare rättigheten genom GDPR? Om en organisation eller annan aktör hanterar någons personuppgifter så skall detta vara tydligt för den som har sina personuppgifter där, vad som behandlas och att det behandlas. Insamling av personuppgifter måste ske på laglig väg. Ett av sätten att samla in personuppgifter kan vara via avtal på olika sätt. Rätt till radering är en del av GDPR och detta innebär att man har rätt att ta bort personuppgifter som behandlas hos en personuppgiftsansvarig. Det som krävs för att bli raderad från ett register är att personuppgifterna inte längre behövs eller måste behandlas av andra orsaker så som lagliga krav eller intresseavvägning. Det finns ett visst antal personuppgifter som absolut inte får behandlas. Dessa personuppgifter är ras, politiska åsikter, religiösa eller filosofiska övertygelser, hälsa, sexualliv eller sexuell läggning. En fysisk person kan inte vara en personuppgiftsansvarig utan det är en organisation. Ett undantag är då en enskild firma har startats, då blir firmaägaren personuppgiftsansvarig. Vid ett samtycke så skall det vara en tydlig handling och inga dolda budskap. Det skall vara tydligt för de som innefattar samtycket att de samtycker och vad de samtycker till. Vid ett eventuellt intrång och personuppgifter kan vara skadade eller överförda till obehöriga så skall en anmälan göras till tillsynsmyndigheten inom 72 timmar. En annan rättighet som kommer med GDPR är medborgares rätt till sin information. Detta innebär att de personuppgifter som behandlas skall beskrivas och lämnas ut till den som söker efter det och detta skall ske utan kostnad. Om man inte följer eller håller GDPR och dess regler så kan man få en straffavgift upp till 20 000 000 EUR.
EU har skapat ett nytt direktiv nämligen NIS. Detta skall ta i beaktning av EU:s medlemsländer. Detta direktiv är skapat för att få en säkrare och tryggare standard inom nätverk- och informationssystem. NIS gäller samhällsviktiga tjänster så som vatten, infrastruktur och mer därtill, det kommer även att gälla digitala tjänster. En digital tjänst kan vara nätbutiker, sökmotorer eller en molntjänst. Om organisationen har en årsomsättning på 10 000 000 EUR, mer än 50 anställda och har sitt huvudkontor i Sverige så gäller NIS som är reglerat i Sverige. I Sverige har vi tillsynsmyndigheter som har olika områden att ansvara för. Om det händer en incident inom en tillsynsmyndighets område skall en incidentrapport skickas. Några av dessa tillsynsmyndigheter och deras ansvarsområden är digital infrastruktur och digitala tjänster som hör till tillsynsmyndigheten Post- och telestyrelsen, sedan har vi också leverans och fördelning av vatten som Livsmedelsverket är tillsynsmyndighet för. Som tidigare beskrivit finns det fler än dessa tillsynsmyndigheter. Det

finns krav som ställs på de organisationer som måste följa NIS. Dessa krav är bland annat att ha gjort ett förberedande arbete för att stärka försvaret vid en eventuell cyberattack. Tanken med detta är att göra en eventuell attack mindre skadlig eller i bästa fall ingen skada alls. Om en incident har inträffat skall en incidentrapport skickas till CSRIT-enheten inom en rimlig tid. CSRIT är ett incidenthanteringsorgan och dess uppgift är att ta emot incidenter rörande IT. Dessa incidenter skall diskuteras inom de andra CSRIT-enheter inom EU. Detta skall medfölja att EU:s medlemsländer skall stötta varandra och hjälpa varandra för att skydda EU som helhet. Tillsynsmyndigheten för området där incidenten inträffat har fortfarande ansvaret för incidenten. CSRIT skall ha alla incidenter för att kunna få en helhetsbild av alla incidenter för att kunna se den större bilden av alla incidenter.
Projektet som skapats i detta arbete var att göra en enkel hemsida där användare kan mötas upp och träffa andra med samma intresse eller träffa de som befinner sig i samma livssituation. Funktionerna är att anmäla sig till en kö där man skriver in stad och intresse. När just den kombinationens kö har fyllts med tio användare så skall en träff skapas, exempelvis på en restaurang. Där skall användare kunna träffa nya bekantskaper eller prata om deras intresse eller om livet. För att arbetets enkla hemsida eller andra hemsidor skall följa reglerna som innefattas av GDPR och NIS så krävs att man tänker på minst följande beskrivning. När det gäller GDPR så handlar det om att hantera andras personuppgifter. Detta skall ske med respekt av informationen man behandlar. Användaren skall veta vad och varför personuppgifterna behandlas. Vid en eventuell registrering av projektets hemsida eller annan hemsida så krävs det en ålderskontroll och ett samtycke. Samtycket innebär att båda parterna går med på att personuppgifter behandlas med respekt och i symbios med GDPR. En organisation som tillhandahåller sökmotorer, köp- och säljtjänster och molntjänst kan absolut behöva anpassa sig inför NIS. Förutom att hemsidan tillhandahåller tjänsterna som radades upp precis så finns det vissa krav för att behöva anpassa sig till NIS, dessa kraven har beskrivits tidigare i detta stycket. I regel är en enkel hemsida likt den som finns med i detta arbetet inget som berörs av NIS.
Det finns uppgifter inom detta examensarbetet som inte hunnits med att fullborda. Det handlar om den automatiska mailfunktionen på hemsidan och att göra hemsidan till HTTPS. Den automatiska mailfunktionen var tänkt att skicka ett mail när en kvot på tio personer är uppfylld och sedan skickas ett mail till exempelvis en restaurang för att boka ett bord för dessa människor. I arbetets slut så blir det ägaren som får skicka mailen manuellt tills dess att denna funktionen är ordnad som det är tänkt. Den andra delen som inte hunnits med att göra är att hemsidan skall vara HTTPS, alltså en säker hemsida. Detta är självklart prioritet ett av dessa två icke avklarade delar. Här är en länk till hemsidan som har skapats i detta arbetet skolaexamen.se.

8.1. Slutsatser

Det är inte så svårt att följa GDPR när man tillhandahåller en hemsida. Det är mest självklara saker som man bör tänka på. Respektera andras personuppgifter och sprid dem inte utan tillåtelse! Att vara tydlig är en bra regel enligt detta arbetets information. Berätta att personuppgifter kommer att sparas och berätta även hur uppgifterna kommer användas! Självklart behöver ingen hantera personuppgifter om det inte finns någon anledning till det. Genom GDPR så har medborgare fått en större rättighet att befoga över dem. Försök inte förhindra det möt istället kraven med öppenhet! Om man väljer att ta hänsyn till GDPR och

dess regler så minskar risken för avgifter som kan bli väldigt dyrt.
När det gäller NIS är det ett bra initiativ från EU att styrka medlemsländers cybersäkerhet. Detta gör att länderna inom EU och medborgarna utan att veta om detaljer får en säkrare tillvaro. Dessa två regleringar från EU är ett bra beslut. Det styrker och skänker trygghet i samhället och för dess invånare. Skyddar mot framtida och nutida hot. Det är inte säkert att de kan skydda från alla hot men de gör ett starkare försvar.

8.2. Fortsatt arbete

Ett fortsatt eller framtida arbete skulle kunna vara om det kommer något som skall ersätta GDPR eller NIS i framtiden. Det kan komma nya förordningar eller direktiv från EU som skall börja gälla istället för GDPR och NIS. Då skulle man kunna ha detta arbetet för att jämföra vad som gäller idag emot det som skulle kunna komma att gälla i framtiden. Med detta sagt så är detta arbetet inte heltäckande av varken GDPR eller NIS så att fullständigt ha detta arbetet som en källa fungerar inte. Däremot för dessa undersökningarnas områden och fördjupningar kan man absolut använda sig av denna informationen för att kunna göra ett fortsatt arbete i framtiden. Vad gäller hemsidan så finns det inte så mycket att jobba vidare på eftersom det inte finns någon kod att fortsätta jobba på. Det som detta arbetet visar på är att det går att göra en enkel hemsida med hjälp av information som finns på internet och på så sätt kan en fortsättning efter man läst detta arbetet vara att skapa en hemsida för egen skull och då kolla ännu närmare på just GDPR för att vara säker på att detta arbetet fått med alla viktiga delar. Det kommer säkert ske förändringar inom GDPR och NIS så en fortsättning skulle kunna vara att uppdatera den nya informationen som kommer in för att få en mer exakt och korrekt information.

9. Referenser

Bolagsverket 2014-13-03, Bolagsverket, åtkomst vid: http://bolagsverket.se/ff/foretagsformer/enskild/vad-1.1971, (2018-05-05).

Datainspektionen (2016) *Dataskyddsförordningen General Data Protection Regulation (GDPR)*, svensk version 679. Europeiska unionens officiella tidning.

Datainspektionen (2016) *Dataskyddsförordningen General Data Protection Regulation (GDPR)*, svensk version 679. Europeiska unionens officiella tidning.

Datainspektionen (2016) *Dataskyddsförordningen General Data Protection Regulation (GDPR)*, svensk version 679. Europeiska unionens officiella tidning, s.36 artikel 39.

Datainspektionen (2017-09-28), Datainspektionen, åtkomst vid: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsbitrade-och-bitradesavtal/, (2018-05-10).

Datainspektionen, Datainspektionen, åtkomst vid: https://www.datainspektionen.se/dataskyddsreformen/, (2018-05-15).

Datainspektionen (2016) *Dataskyddsförordningen General Data Protection Regulation (GDPR)*, svensk version 679. Europeiska unionens officiella tidning, s.6 stycke 32.

Datainspektionen (2016) *Dataskyddsförordningen General Data Protection Regulation (GDPR)*, svensk version 679. Europeiska unionens officiella tidning, s. 16-17 stycke 85-86.

Datainspektionen (2017-04-19), Datainspektionen, åtkomst vid: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-information/, (2018-05-18).

EUR-Lex, (1995), eur-lex, åtkomst vid: https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A31995L0046 , (18-05-05).

Europeiska Unionen, (2018), *europa*, åtkomst vid: (https://europa.eu/european-union/eu-law/legal-acts_sv), (18-05-02).

Myndigheten för samhällsskydd och beredskap, Myndigheten för samhällsskydd och beredskap, åtkomst vid: https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/, (2018-05-20).

Regeringskansliet, (2018-04-06), Justitiedepartementet och Regeringen, åtkomst vid: https://www.regeringen.se/rattsdokument/proposition/2018/04/prop.-201718205/, (2018-05-17).

SFS 2010:1969, Personuppgiftslagen, 5a §.
Datainspektionen (2017-06-29), Datainspektionen, åtkomst vid: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsansvarig/, (2018-05-15).

soi2014, 2014, svenskarna och internet 2014, åtkomst vid: http://www.soi2014.se/den-mobila-boomen-fortsatter/allt-mer-tid-agnas-at-smartmobilen/, (2018-05-20).

Statens offentliga utredningar SOU:2017:36. *Informationssäkerhet för samhällsviktiga och digitala tjänster*, Bilaga 2 s.1.

Statens offentliga utredningar SOU:2017:36. *Informationssäkerhet för samhällsviktiga och digitala tjänster*, Bilaga 2 s.1-2 stycke 1-4.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s.167 kapitel 8.5.2.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, bilaga 1, s.310-312.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s.49.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s.50, kapitel 3.2.1.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, bilaga 2, s.5.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s.128-130.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s.84.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s.96.

Statens offentliga utredningar SOU:2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, s.111.

Wikipedia, responsiv, 2014-10-04, åtkomst vid: https://sv.wikipedia.org/wiki/Responsiv_webbdesign, (2018-05-05).

Wikipedia, HTTPS, 2017-09-11, åtkomst vid: https://sv.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure, (2018-05-06).