En bakgrund till hanterandet av personuppgifter i Piratpartiet

Innehållsförteckning

Syfte med detta dokument

Det tidiga syftet med detta dokument var att skapa ordentliga riktlinjer för vilka som ska ha accesser och vilka accesser dessa ska ha. Även hur vi ska avgöra vilka som ska ha dessa accesser, vilka som har det idag och vad för olika behörigheter som finns. Riktlinjer för vilka som får dela ut accesser var även det en sådan sak som lyftes.

Det fanns även en önskan att tydliggöra vad medlemsservice har för mandat kring att ordna med medlemskap i de lokala föreningarna och likaså vad som gäller för medlemskap inom föreningar när man inte bor inom dess verksamhetsområde.

I arbetet med detta blev det blev tydligare och tydligare ju mer arbete som lades ner att det var många saker som vi inte hade räknat med eller insåg behövdes göras. Av denna anledning har detta dokument därför istället blivit en bakgrund till vidare arbete och diskussion kring arbetet med accesser och hantering av medlemsregistret.

Inga medlemmar namn kommer att figurera i detta dokument.

Hur blir man medlem i Piratpartiet?

På hemsidan www.piratpartiet.se kan man blir medlem i Piratpartiet.

Man fyller i sina uppgifter. Den informationen som anges till den som fyller i uppgifterna är denna text:

> "Dina personuppgifter lagras i ett medlemsregister som hanteras av Piratpartiets funktionärer där du bor och av systemets administratörer, som kan vara aktiva i piratpartier i andra länder. Normalt anonymiseras dina uppgifter tre månader efter ditt medlemskap gått ut. Undantaget är om du varit inblandad i partiets ekonomi, då måste vi spara uppgifterna i tio år för Skatteverkets räkning."

PirateWeb

Medlemmarnas uppgifter samlas i PirateWeb eller PW som det kallas mer internt.

PW är en strukturerad databas för att samla uppgifter om partiets medlemmar. Här ligger även uppgifter kring budget, bokföring, utbetalning av löner osv. Partiet använder PW till en mängd olika uppgifter som rör partiet och inte bara dess medlemsregister.

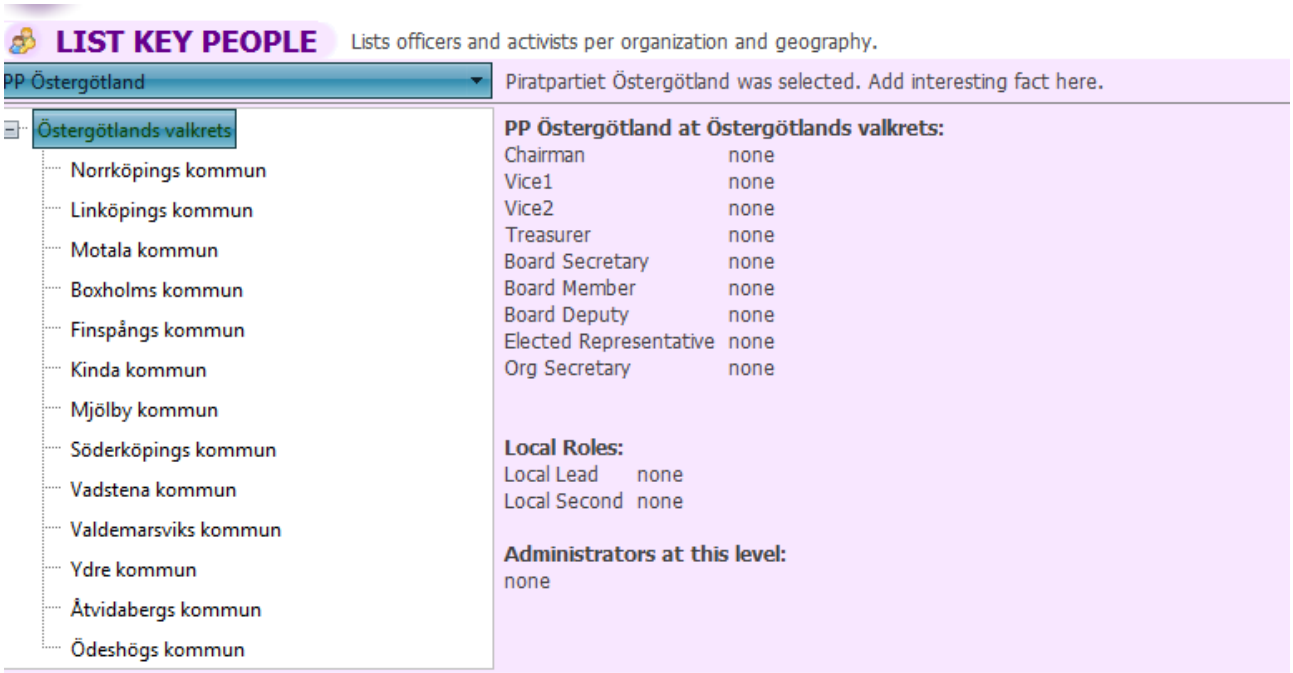
Det går att se vilka roller som finns i PW och vilka behörigheter dessa roller har.[1]

1 https://pirateweb.net/Pages/v4/admin/EditPermsGrid.aspx

Permissions

	Organization																		System		Local					Private	Unknown
	Chairman	Vice1	Vice2	Treasurer	Secretary	Board Member	Board Deputy	Admin	Clerk	Auditor	Member Service	Member Service Lead	Elected Representative	Economy Assistant	Meeting Official	Board Secretary	Local Coordinator	Mail Sender	Admin	Geography Editor	Lead	Deputy	Active	Admin	Election Support	Individual	
CanSeeSelf	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐	☑	☑	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☐	☑
CanSeePeople	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐	☐	☑	☐	☐	☐	☑	☐	☑	☑	☑	☑	☐	☐	☐
CanEditPeople	☑	☑	☑	☑	☑	☐	☐	☑	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☐	☑	☐	☐	☐
CanViewMemberships	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☑	☑	☐	☐	☐
CanEditMemberships	☑	☑	☑	☐	☑	☐	☐	☑	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☐	☑	☐	☐	☐
CanSendLocalMail	☑	☑	☑	☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☑	☐	☑	☑	☐	☑	☐	☐	☐
CanSetUpAutomail	☑	☑	☑	☐	☑	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☑	☐	☑	☐	☐	☑	☐	☐	☐
CanHandlePress	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☐	☑	☐	☐	☐
CanSendGlobalMail	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanSeeEconomyDetails	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanSeeBudget	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☑	☐	☑	☑	☐	☑	☐	☐	☑
CanDoBudget	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanSeeEconomyTransactions	☑	☑	☑	☑	☑	☑	☑	☐	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanDoEconomyTransactions	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanPayOutMoney	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanListOrg	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditOrg	☑	☐	☐	☐	☑	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanSeePoll	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☑	☑	☐	☐	☑
CanEditPoll	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditGeography	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☐
CanValidateActivistEmail	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditMemberSubscriptions	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐
CanEditPermissions	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditOrganisationalRoles	☑	☑	☑	☑	☑	☑	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditSystemRoles	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditLocalRoles	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☑	☑	☐	☐	☐
CanSeeSysadminMenu	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanSeeNonMembers	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditMailTemplates	☑	☐	☐	☐	☑	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanSeeInsensitivePaperLetters	☑	☑	☑	☑	☑	☐	☐	☑	☐	☑	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☑	☑	☑	☑	☐	☐	☐
CanSeeSensitivePaperLetters	☑	☑	☑	☑	☑	☐	☐	☑	☐	☑	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanBreachPostalSecretPaperLetters	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
CanManagePayroll	☑	☑	☑	☑	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanUploadReceivedDocuments	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanEditMailDB	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
CanValidatePolls	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
CanSeeExpiredDuringGracePeriod	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☑	☑	☐	☐	☐	☑	☐	☐	☑	☐	☑	☐	☑	☐	☐	☐	☐
CanMonitorMemberships	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☑	☑	☐	☑	☐	☐	☐
CanMonitorRoleAssignments	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☑	☑	☐	☑	☐	☐	☐

Det går även att gå in i en sökfunktion för att se vilka medlemmar som har olika roller i systemet.[2] Exemplet nedan används för att det inte fanns några medlemmars namn på någon av rollerna.



2 https://pirateweb.net/Pages/v4/Pirates/ListKeyPeople.aspx

Värt att notera

Det finns en roll som heter ”Unknown” som har behörighet att ”Can See Self”, ”Can See Budget” och ”Can See Poll”. Det är oklart om någon har den behörigheten och vad den är till för.

Det är skillnad på Piratpariet SE at [insert stad] och att klicka sig in på den valkretsen och sedan kommunen. Exempel på sådana skillnader är Höörs Kommun. Om man är inne på PP Skåne at Höörs Kommun så finns en person som Chairman och inga andra roller verkar fyllda. Går man istället in på Piratpartiet SE at Höörs Kommun så kan man se att det finns en Administratör på den nivån som inte angavs på den första. Det finns några sådana skillnader med behörigheter som är bör ses över.

Vad är en personuppgift?

Enligt Datainspektionens faktabroschyr är en personuppgift följande:

> Med personuppgift menar man all slags information som direkt eller indirekt kan kopplas till en fysisk person som är i livet. Det är inte bara namn, adress, personnummer och bilder som är personuppgifter. Även uppgifter som indirekt kan kopplas till en person räknas som personuppgifter, till exempel anställningsnummer, kundnummer, bilnummer eller andra kodnummer. Krypterade uppgifter är också personuppgifter så länge någon kan göra uppgifterna läsbara och därmed identifiera individer. Även bild- och ljuduppgifter som kan kopplas till fysiska personer är personuppgifter.[3]

En personuppgiftsansvarig är den som bestämmer varför man ska behandla en personuppgift och även hur. Det kan vara allt ifrån en myndighet eller kommun till en organisation eller ett företag.[4]

Bestämmelser kring PUL och datalagring – kort genomgång

Ett register får inte innehålla mer information än vad som behövs för att fylla registrets ändamål.[5] Uppgifter som inte längre fyller registrets ändamål ska gallras bort.[6] Exempelvis så ska uppgifterna för en medlem som gått ut partiet gallras bort från medlemsregistret om det inte finns särskilda statistiska anledningar att ha kvar uppgifterna varpå endast de uppgifterna som behövs för det ändamålet ska ligga kvar.

Personuppgiftslagen anger även att du som användare/medlem har rätt att få veta vad som finns registrerat av dig. Man har alltid rätt att kostnadsfritt be om ett skriftligt registerutdrag en gång om året. Det ska vara personen tillhanda inom en månad från ett en skriftlig begäran har lämnats in. Här har man även rätt att få veta var uppgifterna kommer ifrån, vad som är ändamålet med registret och till vem eller vilka som uppgifterna lämnats ut till.[7]

Om det visar sig vara några felaktigheter så måste de felaktigheterna på begäran genast rättas, blockeras (spärras) eller raderas ur systemet/registret. Det kan vara allt som är fel eller ofullständigt när det gäller ändamålet för behandlingen. Om den som är registrerad har kränkts eller skadats av felaktigheten eller behandlingen så ska denna ersättas av den personuppgiftsansvarige.[8]

---

3 http://www.datainspektionen.se/Documents/faktabroschyr-personregistrering.pdf s.4 (2014-01-17)
4 http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/dina-rattigheter/ (2014-01-17)
5 http://www.datainspektionen.se/Documents/faktabroschyr-personregistrering.pdf s.5 (2014-01-17)
6 Ibid. s.6
7 Ibid. s.6-7
8 Ibid. s.7

Normalt så gäller inte offentlighetsprincipen inte för föreningar, stiftelser eller privata företag, men den registrerades rätt att få se sina egna uppgifter gäller fortfarande.[9]

Om Datainspektionen kan konstatera att man behandlar personuppgifter på ett olagligt sätt så kommer de i första hand att påpeka detta och ge en möjlighet att åtgärda problemet. Om man däremot inte vidtar de åtgärder som krävs så kan Datainspektionen vid vite förbjuda fortsatt hantering av personuppgifter.[10] I värsta fall kan det bli tal om skadestånd:

> Om personuppgifter har behandlats i strid med personuppgiftslagen och detta har lett till skada eller kränkning av den personliga integriteten ska den personuppgiftsansvarige ersätta den registrerade. Den registrerade har inte bara rätt till ersättning för sakskada, personskada och ren förmögenhetsskada, utan kan även få kompensation för själva kränkningen.[11]

Genomgång av de olika partierna

Datainspektionen gjorde under 2011-2012 en grundlig granskning kring hanteringen av personuppgifter av alla politiska partier med mandat i riksdagen. Den var färdig 7 juni 2012 och publicerades på Datainspektionens hemsida. Den visar på bristande kunskaper om personuppgiftslaget hos samtliga partier.[12]

Datainspektionen menar att de politiska partierna har en omfattande hantering av medlemmars personuppgifter där det inte bara innefattar att behandla känsliga personuppgifter såsom vilka som är medlemmar utan även att det förekommer att de behandlar uppgifter om personer som tagit kontakt med partiet för att få information. Enligt 13§ personuppgiftslagen är uppgiften att någon är medlem i ett politiskt parti en känslig personuppgift. Därför ställs det särskilda krav för hur man skyddar dessa uppgifter.[13]

> Enligt 17 § personuppgiftslagen får ideella organisationer med politiskt syfte inom ramen för sin verksamhet behandla känsliga personuppgifter om organisationens medlemmar och andra personer, som på grund av organisationens syfte, har regelbunden kontakt med den. Känsliga personuppgifter kan också behandlas med den registrerades samtycke.[14]

För att se mer exakt vad varje paragraf innebär kan man slå upp dessa i PUL som finns på Riksdagens hemsida.[15]

Centerpartiet[16]

- Man har inte fullt ut fyllt de krav som ställs i 23-25 §§ personuppgiftslagen när man har lämnat ut information till medlemmarna.
- Lever inte upp till kravet enligt 31§ personuppgiftslagen då man kan komma åt personuppgifter i det centrala registret med enbart användarnamn och lösenord på öppet nät. Det går heller inte att se

9 http://www.datainspektionen.se/Documents/faktabroschyr-personregistrering.pdf s.8 (2014-01-17)
10 http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/dina-rattigheter/ (2014-01-17)
11 Ibid.
12 http://www.datainspektionen.se/press/nyheter/2012/datainspektionen-klar-med-granskning-av-politiska-partier/ (2014-01-17)
13 Bakgrunden finns i samtliga pdf-filer kring genomgång av de politiska partierna. Exempelvis i Kristdemokraternas genomgång: http://www.datainspektionen.se/Documents/beslut/2012-06-07-kd.pdf s.2-3 (2014-01-15)
14 http://www.datainspektionen.se/Documents/beslut/2012-06-07-centern.pdf s.2 (2014-01-17)
15 http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/?bet=1998:204 (2014-01-16)
16 http://www.datainspektionen.se/Documents/beslut/2012-06-07-centern.pdf (2014-01-17)

vem som har tillgång till vilka personuppgifter och när de har haft denna tillgång. Det går heller inte att se vem som har ändrat eller raderat personuppgifter eller när detta har hänt.

Datainspektionen lägger även särskild vikt vid att det inte ska gå att härleda någon information tillbaka till en tidigare medlem som valt att gå ut partiet och att det inte finns någon anledning att det ska behöva göras i slutet av året och inte direkt när detta sker. Detta krävs för att uppgiften ska vara helt avidentifierad. Uppgifter kan sparas för statistiska ändamål men ska då uppfylla de krav som PUL ställer för just statistisk information.

Kristdemokraterna[17]

- Man har inte fullt ut fyllt de krav som ställs i 23-25 §§ personuppgiftslagen när man har lämnat ut information till medlemmarna.
- Hur man har behandlat uppgifter om tidigare medlemmar strider mot 13§ personuppgiftslagen. Detta när det saknats stöd om det i 15-19§§ personuppgiftslagen.
- Lever inte upp till kravet enligt 31§ personuppgiftslagen då man kan komma åt personuppgifter i det centrala registret med enbart användarnamn och lösenord på öppet nät. Vidare skickas medlemsuppgifter i okrypterade filer som bilaga i e-postmeddelanden till ett tryckeri. Ansökan om medlemskap förs från webformuläret till webbservern utan kryptering. Det går heller inte att se vem som har tillgång till vilka personuppgifter och när de har haft denna tillgång. Det går heller inte att se vem som har ändrat eller raderat personuppgifter eller när detta har hänt.
- Man måste upphöra att behandla uppgifter om personer som inte är medlemmar längre eller på något sätt inhämta samtycke till att de får fortsätta behandla dessa uppgifter.

Datainspektionen lägger här särskild vikt vid att man ska upprätta ett skriftligt personuppgiftsavtal med andra som kan ta del av de personuppgifter som finns i medlemsregistret. I det här fallet handlar det om att man skickar uppgifter till ett tryckeri så att de kan skicka ut en medlemstidning.

Miljöpartiet[18]

- Man har inte fullt ut fyllt de krav som ställs i 23-25 §§ personuppgiftslagen när man har lämnat ut information till medlemmarna. Man saknar även rutin för att informera om hur man behandlar personuppgifter för andra än de som är medlemmar.

Moderaterna[19]

- Man har inte fullt ut fyllt de krav som ställs i 23-25 §§ personuppgiftslagen när man har lämnat ut information till medlemmarna.
- Hur man har behandlat uppgifter om tidigare medlemmar strider mot 13§ personuppgiftslagen när det gäller ändamålet återvärvning. Detta när det saknats stöd om det i 15-19§§ personuppgiftslagen. Behandlingen kring personuppgifter för uteslutna strider även det emot 15-19§§ personuppgiftslagen.
- Man måste upphöra att behandla uppgifter om personer som inte är medlemmar längre eller på något sätt inhämta samtycke till att de får fortsätta behandla dessa uppgifter.

17 http://www.datainspektionen.se/Documents/beslut/2012-06-07-kd.pdf (2014-01-15)
18 http://www.datainspektionen.se/Documents/beslut/2012-06-07-mp.pdf (2014-01-16)
19 http://www.datainspektionen.se/Documents/beslut/2012-06-07-m.pdf (2014-01-17)

Socialdemokraterna[20]

- Man har inte fullt ut fyllt de krav som ställs i 23-25 §§ personuppgiftslagen när man har lämnat ut information till medlemmarna.
- Hur man har behandlat uppgifter om tidigare medlemmar strider mot 13§ personuppgiftslagen när det gäller ändamålet återvärvning. Detta när det saknats stöd om det i 15-19§§ personuppgiftslagen. Behandlingen kring personuppgifter för uteslutna strider även det emot 15-19§§ personuppgiftslagen.
- Att man utelämnar uppgifter till A-lotterierna AB strider mot 17§ personuppgiftslagen.
- Lever inte upp till kravet enligt 31§ personuppgiftslagen då man kan komma åt personuppgifter i det centrala registret med enbart användarnamn och lösenord på öppet nät. Det går heller inte att se vem som har tillgång till vilka personuppgifter och när de har haft denna tillgång. Det går heller inte att se vem som har ändrat eller raderat personuppgifter eller när detta har hänt.

Sverigedemokraterna[21]

- Man har inte fullt ut fyllt de krav som ställs i 23-25 §§ personuppgiftslagen när man har lämnat ut information till medlemmarna. Vidare saknas det rutiner och information för att informera de som inte är medlemmar hur deras uppgifter registreras.
- Hur man har behandlat uppgifter om tidigare medlemmar strider mot 13§ personuppgiftslagen när det gäller ändamålet återvärvning. Detta när det saknats stöd om det i 15-19§§ personuppgiftslagen. Behandlingen kring personuppgifter för uteslutna strider även det emot 15-19§§ personuppgiftslagen.
- Lever inte upp till kravet enligt 31§ personuppgiftslagen då man kan komma åt personuppgifter i det centrala registret med enbart användarnamn och lösenord på öppet nät. Det går heller inte att se vem som har tillgång till vilka personuppgifter och när de har haft denna tillgång. Det går heller inte att se vem som har ändrat eller raderat personuppgifter eller när detta har hänt.

Vänsterpartiet[22]

- Man har inte fullt ut fyllt de krav som ställs i 23-25 §§ personuppgiftslagen när man har lämnat ut information till medlemmarna. Vidare saknas rutiner för att informera prenumeranter till deras tidning hur personuppgifterna hanteras kring att distribuera tidningen.
- Hur man har behandlat uppgifter om tidigare medlemmar strider mot 13§ personuppgiftslagen när det gäller ändamålet återvärvning. Detta när det saknats stöd om det i 15-19§§ personuppgiftslagen.

Sociala Medier

Partiet ansvarar även för personuppgifter som läggs ut på sociala medier. Vi är ansvariga för den information vi själva lägger ut på våra facebook-sidor och på våra bloggar men även den informationen som andra publicerar på dessa ställen. Den som har skrivit kommentaren kan också ha ett ansvar för uppgiften den har publicerat. På Twitter så ansvarar organisationer endast för uppgifter vi själva publicerar, inte sådant som andra publicerar eftersom det är inget som man kan ha kontroll över.[23]

20 http://www.datainspektionen.se/Documents/beslut/2012-06-07-sap.pdf (2014-01-16)
21 http://www.datainspektionen.se/Documents/beslut/2012-09-07-sd.pdf (2014-01-17)
22 http://www.datainspektionen.se/Documents/beslut/2012-06-07-vp.pdf (2014-01-17)
23 http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sociala-medier/ (2014-01-17)

När det gäller andra sociala medier som organisationen använder så är det organisationen själv som måste göra en avvägning kring vilket ansvar som organisationen har. Tumregel är att om organisationen kan ansvara för vad som publiceras på deras sidor så har organisationen ett ansvar även för vad andra publicerar och annars har organisationen ett ansvar för det som de själva publicerar.[24]

Organisationen är skyldig att vidta de åtgärder som behövs för att det inte ska publiceras kränkande personuppgifter på de sociala medier som organisationen har. Sådana uppgifter kan leda till skadestånd om de får ligga kvar.[25]

Piratpartiet har idag ett officiellt Twitter-konto, en officiell Facebook-sida, en officiell Facebook-grupp, ett officiellt Google+-konto och Piratpartiets hemsida som är uppbyggd som en samling bloggar där andra kan kommentera på inlägg. Det finns även ett antal fler sajter som partiet har officiella eller halvofficiella konton såsom youtube, bambuser osv. Det finns en rad användare som har tillgång till dessa olika konton.

Dessa bestämmelser förutsätter att man inte för något slags register kring de personuppgifter som finns på de sociala medierna. I de fallen så gäller personuppgiftslagen i sin helhet.[26]

Åtgärder som redan implementerats

Det finns en åtgärd som redan har implementerats på olika delar av tillgången till medlemsregistret och det är tvåfaktorsautentisering.

Det innebär att det behövs två faktorer för att få tillgång till vissa delar av medlemsregistret istället för endast en. Förr räckte det med att någon som hade behörighet loggade in i PW och hade därifrån behörighet att se hela eller delar av medlemsregistret. Nu måste man även autentisera sig med en kod man får genom google authenticator eller via sms.

Dvs för att få tillgång till medlemsregistret så behöver man både ha sitt lösenord (något som bara användaren kan) och en kod (något som bara användaren har).

Wikipedia förklarar det på följande sätt:

> Two-factor authentication is often confused with other forms of authentication.
> Two-factor authentication requires the use of two of the three authentication factors.
> The factors are identified in the standards and regulations for access to U.S.
> Federal Government systems. These factors are:
> Something only the user knows (e.g., password, PIN, pattern);
> Something only the user has (e.g., ATM card, smart card, mobile phone); and
> Something only the user is (e.g., biometric characteristic, such as a fingerprint).[27]

24 http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sociala-medier/ (2014-01-17)
25 Ibid.
26 Ibid.
27 http://en.wikipedia.org/wiki/Multi-factor_authentication (2014-01-17)

Hur går vi vidare?

Detta dokument visar på en bakgrund till de åtgärder som Piratpartiet skulle behöva göra för att säkerställa att PUL följs och att alla delar av medlemsregistret och hanteringen av detta sköts som det ska.

Om Datainspektionen i nuläget skulle utreda oss vet vi att vi kommer få möjlighet att rätta till det om de anser att det finns saker vi inte följer till fullo. Hur mycket det är vet vi inte just nu utan är något vi får jobba vidare med för att åstadkomma.

Konkreta saker som behöver göras:

- Skriva en policy för hanteringen av sociala media med information och instruktioner kring hanteringen av dessa i relation till PUL.
- Skriva en IT-säkerhetspolicy där man i detalj listar både roller, accesser och hanterandet av dessa. Även hur man ska hantera allmän IT-säkerhet inom partiet. Här ska det även ingå vilka som ska ha rättigheter i medlemsregistret och varför.
- Skapa en IT-utbildning till funktionärer med syfte att lära dem om IT-säkerhet, PUL och hanteringen av medlemsregistret.
- Göra en grundlig genomgång av hur systemet och rutinerna fungerar idag och vad som behöver ändras för att kunna jobba i enlighet med PUL och vår framtida IT-säkerhetspolicy.

Partiledningen bör fortsätter arbetet med detta för att så snart som möjligt ha policys och liknande färdigt att implementeras i hela organisationen.