



Tilläggsprotokoll

till 0150-K2050-20

Äklr
AM-63682-20
Signerat av

Enhet

Särskilda utredningar, Utredning 1 Göteborg SU

Handläggare (Protokollförare)

Mats Edsand

Undersökningsledare

Kajsa Sundgren

Polisens diarienummer

0150-K2050-20

Arkiv/Äkl. ex

Signerat av: MÅLSÄGANDEN TINGSRÄTT
Handläggare 5

Datum: 2022-09-30
2022-01-27
AKTBIL: 64

Personer i ärendet

Förtursmål Nej	Beslag	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen Nej
Ersättningsyrkanden		Tolk krävs
Misstänkt (Efternamn och förnamn) Ambjörnsson, Lars Martin		Personnummer 19830922-6234
Brott Dataintrång		
Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats		
Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt Per post	Underrättelse utsänd 2022-01-27	Yttrande senast 2022-02-11
Försvare Mats Hellman, förordnad 2020-11-10	2022-01-27	2022-02-11
Underrättelsesätt, försvare Per post	Resultat av underrättelse mt Erinran, 2022-02-21	Resultat av underrättelse försv Erinran, 2022-02-21

Brott i ärendet

Brottsbeskrivning Dataintrång		
Brottsplatsadress POLISMYNDIGHETEN, Karlstad	Händelse inträffad - - :	Händelse inträffad mellan 2019-06-29 - 2019-06-29
Aktör Ambjörnsson, Lars Martin Larsson, Kenth Robert		Roll Misstänkt Vittne
Brottsbeskrivning Dataintrång		
Brottsplatsadress POLISMYNDIGHETEN, Karlstad	Händelse inträffad - - :	Händelse inträffad mellan 2019-12-06 - 2019-12-06
Aktör Ambjörnsson, Lars Martin		Roll Misstänkt
Brottsbeskrivning Dataintrång		
Brottsplatsadress POLISMYNDIGHETEN, Karlstad	Händelse inträffad - - :	Händelse inträffad mellan 2019-12-03 - 2019-12-03
Aktör Ambjörnsson, Lars Martin		Roll Misstänkt
Brottsbeskrivning Dataintrång		
Brottsplatsadress POLISMYNDIGHETEN, Karlstad	Händelse inträffad - - :	Händelse inträffad mellan 2019-12-03 - 2019-12-03
Aktör Ambjörnsson, Lars Martin		Roll Misstänkt

Notering

Innehållsförteckning

Diariernr	Uppgiftstyp	Sida
	Anmälan	
0150-K2050-20	Anmälan	4
	<i>Bilaga: Ursprunglig anmälan</i>	
	Mejl från mt och försvarare.	
	Mejl från försvarare till åklagare.....	6
	Mejl från försvarare - IT säk.utbildning.....	7
	Mejl från försvarare - MBL.....	8
	Mejl från försvarare - Rapport dataintrång.....	12
	PM ang utb.	
	PM Utbildning.....	28
	Tjänstgöringstider Cops	
	Tjänstgöring 2019-06-29.....	29
	Tjänstgöring 2019-12-03 och 2019-12-06.....	32
	PM Frånvarokoder i Cops.....	36
	Sekretessinformation mt	
	Sekretessinformation Martin Ambjörnsson 2010-01-26.....	37
	Pm utbildning	
	Mejl från GSD ang Ambjörnsson.....	38
	PM 2017:4	
	PM 2017:4.....	40
	Finns önskemål om ytterligare information eller förhör önskar åklagare få reda på detta.	
	Personalia	
	Bilaga skäligen misstänkt, Ambjörnsson, Lars Martin.....	47
	Personalia, Ambjörnsson, Lars Martin.....	49

A N M Ä L A N

ARKIVEXEMPLAR
2020-04-30 11.01
0150-K2050-20
Sida: 1

Polismyndigheten
SU

Anm.upptagande p-mynd: POLISMYNDIGHETEN Dnr: 0150-K2050-20
Enhet: 5980AS1 Myndighetskod: 5000 Dnr annan p-mynd: 5000-K503568-20
Anmälningsdatum: 2020-04-29 kl: 15.00 Anmälningssätt: Polisanställd i tjänst
Upptagen av: Inspektör Lars-Göran Bäckman
Inskriven av: Kommissa. Rose-Marie Carina Hagman Ringström
Inskriven: 2020-04-30 kl: 10.33 Handl. p-mynd: SÄRSKILDA UTREDNIN
Enhet: 5980AS1

SAMMANDRAG

MÅLSÄGANDE:
GADDE, BERNE

MISSTÄNKT:

ANMÄLARE:

ÖVRIGT:
Fritext

VITTNÉ:
SÖDER, SOFIA

UTPEKAD JURIDISK PERSON:

BILAGOR:

BROTT/HÄNDELSE

1.40

Brottskod

Tjänstefel

2002

POLISMYNDIGHETEN, KARLSTAD

Länskod: 17

Omrkod:

t.o.m. Onsdag 2020-04-29 kl 15.00

GADDE, ULF ROGER BERNE

Målsägande fysisk

SÖDER, LISA SOFIA

Vittne

FRITEXT

BROTET:

Målsägaren uppgav att han misstänker att en anställd inom Polismyndigheten röjt sekretessbelagda uppgifter om målsägaren till utomstående utanför Polismyndigheten. Uppgifter om att så kan vara fallet har inkommit till målsäganden på olika sätt. Målsäganden har tidigare anmält liknande händelse men valde då att inte tala om vem han misstänkte. Då det inträffade tycks fortsätta så vill han nu fullfölja en ny anmälan. Förutom det vittne som anges i anmälan finns ytterligare vittne. Målsägaren har uppgifter om detta. Det finns även sparade ljudfiler.

Ärendesamordning 1 SU
Box 12256
102 26 STOCKHOLM
Tfn:
E-post:

Besöksadress: Kungsgatan 60
Faxnr: 010-5635662
Handl. enhet: Ärendesamordning 1 SU
Handläggare: Kommissa. R C Hagman Ringström

A N M Ä L A N

ARKIVEXEMPLAR
2020-04-30 11.01
0150-K2050-20
Sida: 2

Polismyndigheten
SU

MÅLSÄGANDE

GADDE, ULF ROGER BERNE Kön: M
Försäkringsbolag:

VITTNÉ

SÖDER, LISA SOFIA Kön: K

Ärendesamordning 1 SU
Box 12256
102 26 STOCKHOLM
Tfn:
E-post:

Besöksadress: Kungsgatan 60
Faxnr: 010-5635662
Handl. enhet: Ärendesamordning 1 SU
Handläggare: Kommissa. R C Hagman Ringström

0150-k2050-20 Mejl från försvarare

Från: Mats Hellman <mats.hellman@werners.se>

Skickat: måndag den 22 november 2021 17:19

Till: Sundgren Kajsa <Kajsa.Sundgren@aklagare.se>

Ämne: Angående åtalet mot Martin Ambjörnsson

Hänvisar till dagens telefonsamtal och bifogar aktuell rapport om it-säkerhetsutbildning och uppgifter om när och vilken utbildning Ambjörnsson genomgått samt protokoll MBL förhandling. Den sistnämnda visar att poliserna riskerar göra omedvetna fel på grund av utbildningsbristerna och att anpassningen till den snabba teknikutvecklingen brister.

Den andra filen visar att Ambjörnsson inte alls var utbildad innan hävdade brottsdatum. Vidare visar rapporten från SU att utbildningen inom polismyndigheten har allvarliga brister och att kontrollen beträffande vilken utbildning respektive polis genomgått också brister. Till detta kommer också att det på grund av utbildningsbristerna sannolikt uppkommit en egen kultur inom polisen om vad man får och inte får göra som inte stämmer med regelverket. Samtidigt menar Ambjörnsson att han uppfattat att det från polismyndigheten uppmuntrats att vara aktiv utanför egen tjänstetid och att man kan göra slagningar för att kontrollera misstänkta händelser eller uppgifter som kommer en till del utanför tjänstetid.

Det kan med andra ord konstateras att Ambjörnsson inte hade någon it-säkerhetsutbildning innan 2020. Han var därför utelämnad åt sig själv och vad han uppfattat när det gäller vad som är tillåtet eller inte. Vidare var han placerad i Stenungssund som områdespolis och hade även tjänstgöring i Uddevalla. I den egenskapen har han mottagit tips som handlat om misstänkt missbruk av vapen, bråk och eventuell misshandel i en familj med barn samt angående ungdomar på glid. Med andra ord var det definitivt fråga om brott och problem som låg inom hans normala arbetsområde. Detta medförde att han gjorde slagningar och kontrollerade uppgifter beträffande aktuella personer eftersom han uppfattade att detta var tillräckligt tjänsterelaterat. Att några slagningar gjordes utanför tjänstetid handlar om att han uppfattade att det inte fanns anledning att vänta och att saken kunde vara brådskande. Dessutom hade han direkt tillgång till registren genom tjänstetelefonen eller att han råkade befinna sig på polisstationen. Sammantaget har Ambjörnsson uppfattat att samtliga slagningar varit tjänsterelaterade och han har inte haft något som helst uppsåt att bryta mot regelverket. Under alla omständigheter måste eventuella felaktiga slagningar skyllas på polismyndigheten och de allvarliga brister som gäller myndighetens it-säkerhetsutbildning och kontrollen av utbildningens genomförande samt att bristerna medfört att det uppstått egna felaktiga tolkningar i brist på tydlighet.

Med hänvisning till ovanstående begärs det att åtalet mot Martin Ambjörnsson omprövas och läggs ned.

Karlstad den 22 november 2021

Mats Hellman

The screenshot shows a web browser window displaying the 'Godk nda aktiviteter' (Approved activities) page on the Polisens website. The page is in Swedish and shows a list of approved activities. The user is logged in as Martin Ambj rnsson.

Godk nda aktiviteter

H r finns alla aktiviteter som du har tillg ng till. Fler aktiviteter kan du hitta i Katalogen. H r visas dina avklarade aktiviteter. Klicka p  aktivitetens namn f r att g  till aktiviteten.

Mina aktiviteter

- Alla (13)
- P g ende (7)
- Dolda (0)
- Godk nda (4)**
- Arkiverade (2)

Roller

- Deltagare (13)

S k aktiviteter

S k p  inneh ll i aktiviteter

Visar: 50 (Totalt 4)

Info	Aktivitet	Ing�r i samlingsaktivitet	Godk�nd	Funktioner
�	ANPR		2020-01-14	
�	Introduktionsutbildning i informations�kerhet		2020-01-10	
�	Mobilit�t - grundutbildning		2021-04-09	
�	Obot - digitala ordningsf�rel�gganden Obot		2021-04-07	

1 (4)

MBL 30/2016

**Polisen**

Datum

2016-06-20

Diariennr (åberopas)

MBL § 11 Polismyndighetens riktlinjer för mobil elektronisk utrustning**Tid:**

tisdag 7 juni 2016

Parter:**Arbetsgiversidan:**

Åsa Hollmén, ordförande (tillika protokollförare)
Ylva Söderlund, IT
Damir Omérov, HR
Daniel Larsson, IT
Fredrik Ringdén, IT

Arbetstagarsidan:

Polisförbundet

Göran Malmberg (delvis) och Fredrik Westin

ST inom Polisen

Pär Renberg

Saco-S

Lars Modig och Anna Lindgren

Seko Polisen

Karna Tillheden och Annika Olsen

Övriga närvarande:

Madeleine Rogersten, sekreterare
Lennart Grönberg NHSO

Ärende: Polismyndighetens riktlinjer för mobil elektronisk utrustning

24
LM (100)
PR VT

2016-06-20

§ 1 Kallelse m.m.

Arbetsgivaren har kallat till förhandlingen. Underlag har skickats ut inför förhandlingen.

§ 2 Justeringspersoner

Till justeringspersoner utsågs för arbetsgivaren ordförande Åsa Hollmén och för respektive arbetstagarorganisation, Polisförbundet Fredrik Westin, ST inom Polisen Pär Renberg, Saco-S Lars Modig och Seko Polisen Karna Tillheden.

§ 3 Arbetsgivarens förslag

It-juridik har tillsammans med it-säkerhet fått i uppgift att ta fram riktlinjer för polisens användande av mobil elektronisk utrustning (främst mobiltelefoner). I riktlinjen tas vissa säkerhetsmässiga och juridiska aspekter upp. I riktlinjen ingår numer även skatterättsliga bestämmelser. Syftet är att alla användare av mobil it-utrustning ska få viss vägledning kring sitt användande av framförallt mobiltelefon men även surfplattor. Mobilitetsgruppen ser ett stort behov av att riktlinjen beslutas i takt med att allt fler polisen i yttre tjänst förses med nya mobiltelefoner med tillgång till polisiära it-system.

§ 4 Synpunkter och frågor från Arbetstagarorganisationerna (ATO)

Polisförbundet framför att riktlinjerna är för otydliga - i synnerhet vad gäller den enskilde medarbetarens ansvar för säkerhetsaspekter m.m. Polisförbundet anser vidare att mobil elektronisk utrustning ska vara ett arbetsredskap som lämnas på arbetsplatsen efter avslutad tjänstgöring – detta för att undvika sammanblandning mellan arbete och fritid. Förbundet påtalar att hantering av Wifi, appar samt Apple-ID inte är reglerat i riktlinjerna med utgångspunkt från användande och säkerhetsaspekter.

Även Seko Polisen anser att riktlinjerna är otydliga vad gäller den enskildes ansvar. Riktlinjerna bör därför förtydligas. Seko Polisen har även frågor rörande säkerhet vid användning av olika appar där det finns risk att obehöriga får del av information om Polisens anställda.

§ 5 Arbetsgivarens svar och kompletteringar utifrån ATO:s frågor och synpunkter

Arbetsgivaren redogör för hur Apple-ID bör hanteras, hur planeringen på kort och lång sikt ser ut vad gäller Wifi-uppkoppling samt vad som gäller avseende användning av olika appar som kräver tillgång till kontaktbok etc.

§ 6 Yrkande från Polisförbundet och Seko Polisen

LM
PR

2016-06-20

Polisförbundet yrkar att riktlinjen ändras så att privat användning av utrustningen inte är tillåten utanför arbetstid. Utrustningen ska enligt förbundet istället lämnas kvar på arbetet efter avslutad tjänstgöring med anledning av de otydliga riktlinjerna som riskerar att medlemmarna bryter mot regelverket och där igenom får stå personligt ansvariga för eventuella felaktigheter.

Riktlinjerna riskerar att skapa en situation där arbetsgivaren bryter mot författnings- och kollektivavtalsreglering kring arbetstid.

Seko Polisen yrkar att förtydliganden av riktlinjerna sker enligt vad som framgår ovan.

§ 7 Arbetsgivarens inställning till framförda yrkanden

Arbetsgivare meddelar att Polisförbundets yrkande ej kan medges eftersom det finns starka önskemål i organisationen om att kunna använda mobil elektronisk utrustning såväl privat som i tjänsten. Ska detta behov tillgodoses måste utrustningen kunna användas även utanför tjänstgöringstid.

Vad gäller Seko Polisen yrkande meddelar Arbetsgivaren att vissa önskade förtydliganden kan göras beträffande den enskilde medarbetarens ansvar för säkerhet m.m.

§ 8 Avslut

Förhandlingen avslutas i enighet med Saco-S och ST inom polisen.

Förhandlingen avslutas i oenighet med Polisförbundet.

Seko Polisen avser meddela sin inställning när de tagit del av de utlovade justeringarna av riktlinjerna.

Förhandlingen anses avslutad med samtliga ATO efter slutlig justering av protokollet.

Den 10 juni meddelar Seko Polisen att de ej anser att arbetsgivarens kompletterande skrivningar i riktlinjerna är tillfyllest varför de avslutar förhandlingen i oenighet.

LM
PR
9/6
PR

2016-06-20

Vid protokollet

Åsa Hollmén

Justeras för Polismyndigheten

2016-06-21



Åsa Hollmén

Justeras 2016-06-20



Pär Renberg

Justeras 2016-06-20



Fredrik Westin

Justeras 2016-06-20



Karna Tillheden

Justeras 2016-06-21



Lars Modig



Rapport effektivisering av utredningsverksamhet gällande dataintrång

Underlag för fortsatt arbete vid SU

Rapport dataintrång

Innehåll

1	SAMMANFATTNING.....	3
2	UPPDRAGET	4
2.1	Bakgrund och syfte	4
2.2	Mål.....	5
2.2.1	Effektmål	5
2.2.2	Produktmål	5
2.3	Förtydliganden och avgränsningar.....	5
2.4	Tidigare arbete	5
3	TILLVÄGAGÅNGSSÄTT OCH ARBETSFORMER.....	6
3.1	Deltagare i arbetsgruppen	6
3.2	Arbetsformer	6
4	RESULTAT.....	6
4.1	Genomgång av nuläget	6
4.1.1	Domar	7
4.1.2	Nedläggningsgrunder.....	8
4.1.3	Befogenhet och styrdokument	8
4.1.4	Utbildning i informationssäkerhet	8
4.1.5	CSL.....	9
4.1.6	PAN	9
4.1.7	Brott mot tystnadsplikt	10
4.1.8	Metodstöd, PNU, m.m.	10
4.2	Beskrivning och analys av den befintliga processen.....	10
4.2.1	Befintliga och framtida hinder och framgångsfaktorer	11
4.3	Förslag till åtgärder.....	12
4.3.1	Kompetenshöjning inom SU.....	12
4.3.2	Gemensamt metodstöd.....	13
4.3.3	Mall från underrättelseenheten	13
4.3.4	Modell för återkoppling.....	14
4.3.5	Samarbete med SÅK.....	14
4.3.6	Särskilt om CSL.....	15
4.4	Förslag till åtgärder inom övriga Polismyndigheten.....	15
5	FÖRSLAG TILL FORTSATT ARBETE.....	16
5.1	Utbildning	16
5.2	Metodstöd	16
5.3	Modell för återkoppling	16
5.4	Övriga åtgärder	16

Dokument
RAPPORTSida
3 (16)

Upprättad av

Datum
2021-09-07Diariennr
A094.823/2021Saknr
129Version
01.01

Denna rapport är framtagen vid avdelningen för särskilda utredningar i syfte att effektivisera utredningar av dataintrång. Den är främst framtagen som ett beslutsunderlag för avdelningschefen och som ett underlag för det fortsatta arbetet att utveckla utredningar av dataintrång.

1 Sammanfattning

Avdelningschefen för särskilda utredningar (SU) Ebba Sverne Arvill beslutade i februari 2021 att tillsätta en arbetsgrupp kring avdelningens utredningsverksamhet rörande dataintrång. Ett projektdirektiv har styrt arbetsgruppens arbete där effektmålet har varit att identifiera framgångsfaktorer och hinder samt lämna förslag som syftar till en ensad och effektiviserad utredningsprocess som reducerar antalet resurstimmar vid handläggning av dataintrång. Detta eftersom dataintrång är ett vanligt förekommande brott som i nuläget tar många resurstimmar i anspråk både för SU:s underrättelse- och utredningsverksamhet.

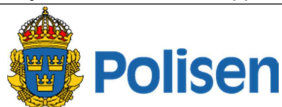
Arbetsgruppen har träffats vid tio digitala möten. Intervjuer har genomförts med SU:s enhetschefer och dialog har hållits med en referensperson vid Särskilda åklagarkammaren (SÅK). Uppdraget har dock varit att fokusera på processen inom utredningsverksamheten vid SU.

Vid en genomgång av nuläget har arbetsgruppen kunna konstatera att det finns faktorer såväl inom som utom SU:s kontroll som försvårar effektiviseringen av processen. Till problembilden hör bland annat att information om och utbildning i informationssäkerhet verkar ha haft svårt att hålla jämna steg med den snabba teknikutveckling som har ägt rum vid Polismyndigheten de senaste åren.

Ett annat dilemma är att genomförda förundersökningar avseende dataintrång läggs ned av åklagare vid SÅK. Den främsta anledningen till detta är otydligheten från Polismyndighetens sida om vad som är otillåtna slagningar. Genom att det finns brister i utbildningen uppstår det inte sällan oklarheter vad gäller uppsåtet. Områden som återkommer gång på gång i samband med misstanke om brott är vad som har varit arbetsuppgiften, vad som ingår i serviceskyldigheten och var gränsen för jäv går.

Med detta som grund har arbetsgruppen tittat närmare på områdena domar, nedläggningsgrunder, befogenhet och styrdokument, utbildning i informationssäkerhet, Centrala säkerhetsloggen (CSL), Personalansvarsnämnden (PAN), (synen på brottsvolym i förhållande till arbetsrättsliga beslut), brott mot tystnadsplikt (brott mot tystnadsplikt i kombination med dataintrång) samt befintliga metodstöd inom ramen för polisens nationella utredningsdirektiv (PNU).

I samband med genomgången av nuläget har arbetsgruppen även identifierat hinder och framgångsfaktorer samt diskuterat hur hinder skulle kunna vändas till framgångsfaktorer. Idag saknas till exempel ett gemensamt metodstöd, vilket gör att arbetssätten varierar och det berömda hjulet riskerar att uppfinnas gång på gång. Enligt arbetsgruppens bedömning är framtagandet av ett gemensamt metodstöd kanske den åtgärd som har den enskilt största potentialen att ensa och effektivisera utredningsprocessen vid SU.

Dokument
RAPPORTSida
4 (16)

Upprättad av

Datum
2021-09-07Diariennr
A094.823/2021Saknr
129Version
01.01

Ökad analytisk förmåga vid utredningsenheterna är ett annat område, som bedöms kunna ge tids- och kvalitetsvinster för utredningsarbetet. Ytterligare exempel på en framtida framgångsfaktor är loggningen av it-systemen. CSL har redan idag en mycket central roll vid utredningen av dataintrång, men arbetsgruppens bedömning är att underlagen har förbättringspotential som kan leda till ökad effektivisering av utredningsprocessen.

I rapporten presenteras ett antal förslag till åtgärder. Bland annat föreslås kompetenshöjning vid avdelningen. Vidare föreslås att ett gemensamt metodstöd tas fram. Arbetsgruppen har påbörjat arbetet och lagt en grund till ett sådant stöd på I:\. På sikt bör det läggas i Durtvå plus. Framtagandet behöver ske i samarbete med SÅK.

Andra förslag till åtgärder är att mallen *Underlag för anmälan om dataintrång* utvecklas och att olika former för återkoppling tillämpas. Som ovan har nämnts behöver även samarbetet med CSL fortsätta att utvecklas i syfte att få lättbegripliga, standardiserade och rättssäkra underlag därifrån.

Under arbetets gång har arbetsgruppen även konstaterat att det finns åtgärder utanför uppdraget och direktivet, som är vitala för arbetet mot dataintrång. Därför föreslår arbetsgruppen ett antal åtgärder som i första hand behöver vidtas av andra delar av Polismyndigheten. Den viktigaste av dessa är att ett samarbetsforum bildas mellan it-avdelningen, verksamhetsskyddet, SU och informationsägare för att kunna åtgärda gemensamma problem, såsom att i olika styrdokument och utbildningar tydliggöra gränsen mellan lovlig och olovlig användning av it-systemen.

Myndigheten skulle dessutom behöva se över sina it-säkerhetsutbildningar samt genomföra behörighetsöversyner.

En annan föreslagen åtgärd, som enligt arbetsgruppens bedömning kan ge stora tids- och kvalitetsvinster för utredningsarbetet, är om respektive informationsägare tar fram ett underlag med beskrivning av systemet med vad som framkommer vid respektive slagning i systemet samt skärmdumpar utvisande hur systemet ser ut och vilka val som kan göras vid slagningar med mera. Ett sådant material är även tänkt att ingå i det gemensamma metodstödet.

I rapporten lämnas slutligen förslag till fortsatt arbete. Bland annat föreslås utbildningsinsatser samt en gemensam arbetsgrupp mellan SU och SÅK, för att med det insamlade materialet som grund ta fram ett gemensamt metodstöd och en grundmall för förundersökningsprotokoll. Arbetsgruppen föreslår även att SU kansli ges i uppdrag att ansvara för att den föreslagna modellen för återkoppling genomförs.

2 Uppdraget

2.1 Bakgrund och syfte

Den 16 februari 2021 beslutade avdelningschefen för SU, Ebba Sverne Arvill om att tillsätta en arbetsgrupp kring avdelningens utredningsverksamhet rörande dataintrång. Detta då dataintrång är ett vanligt förekommande brott både för underrättelse- och utredningsverksamheten inom SU och tar därmed många resurstimmar i anspråk. Arbets-

Dokument
RAPPORTSida
5 (16)

Upprättad av

Datum
2021-09-07Diariennr
A094.823/2021Saknr
129Version
01.01

gruppens uppdrag har dock varit att fokusera på processen inom SU:s utredningsverksamhet. Ett projektdirektiv har styrt arbetsgruppens arbete.¹

2.2 Mål

Ett effektmål och fyra produktmål har styrt arbetet. Nedan följer en beskrivning.

2.2.1 Effektmål

Identifiera framgångsfaktorer och hinder samt lämna förslag som syftar till en ensad och effektiviserad utredningsprocess vid dataintrång och därmed reducera antalet resurstimmar för handläggning.

2.2.2 Produktmål

Uppdraget ska leverera en rapport som innehåller följande fyra delar:

1. Beskrivning och analys av utredningsverksamhetens befintliga processer och rutiner med fokus på identifierade och framtida framgångsfaktorer och hinder.
2. Förslag på en sammanställningsmall som ska bifogas underlag för anmälan från SU Underrättelse i ärenden som avser misstänkta dataintrång.
3. Förslag till ensade och gemensamma åtgärder, behov och rutiner som kan bidra till att effektivisera utredningsverksamhetens arbete med förundersökning gällande dataintrång.
4. Förslag på modell och innehåll för återkoppling av erfarenheter från utredningsverksamheten tillbaka till övriga delar av avdelningen i syfte att kunna förebygga, förhindra och upptäcka aktiviteter som skulle kunna vara kopplad till dataintrång.

2.3 Förtydliganden och avgränsningar

Vid beredning med avdelningschefen den 16 mars gavs förtydligandet att arbetsgruppen skulle omhänderta alla slagningar som görs av polisanställda. Inte bara slagningar i polisens system, eftersom systemägare ibland är en annan myndighet än polisen. Dessutom att uppdraget innefattade slagningar som görs både under arbetstid och på fritiden.

2.4 Tidigare arbete

Vid SU har följande rapporter tagits fram under 2017 och 2019. *Antalsräkning slutrapport* 2019-10-07 där en gemensam arbetsgrupp mellan SU och SÅK resonerade kring antalsräkning för omfattande dataintrång. I rapporten *Modell för anmälningar gällande dataintrång* 2017-04-11 lämnade arbetsgruppen förslag till åtgärder som bland annat handlar om antalsräkning, underlag från CSL, brottsförebyggande åtgärder, utbildning i it-säkerhet samt bättre samarbete mellan SU:s enheter och SÅK.

Ytterligare en rapport som är av intresse i sammanhanget är internrevisionens *Granskning av polisens förmåga att förebygga, upptäcka och hantera oegentligheter i polisens IT-system*². I rikspolischefens vidhängande beslut anges bland annat ”Vidare ska it-avdelningen etablera ett samverkansforum för it-avdelningen, verksamhetsskyddet avdelningen för särskilda utredningar och informationsägare i syfte att förbättra förmågan att upptäcka oegentligheter”. Ett sådant samverkansforum har inte etablerats.

¹ Bilaga 1

² A419.644/2016

Värdet av ett sådant forum torde vara stort för att lösa en del av de åtgärder som anges under avsnitt 4.4 *Förslag till åtgärder inom övriga Polismyndigheten*.

3 Tillvägagångssätt och arbetsformer

3.1 Deltagare i arbetsgruppen

Arbetsgruppen har bestått av följande personer:

Per Blomqvist, sammankallande, kansliet

Lotta Wallén, sekreterare, kansliet

Jessica Solner, utredare, utredningsenheten i Malmö

Asta Kovanen Schüller, analytiker, utredningsenheten i Göteborg

Karin Ljungberg, handläggare, samordningsenheten

Kent Holmstedt, utredare, utredningsenheten i Stockholm

Elin Edblom, handläggare, underrättelseenheten

3.2 Arbetsformer

Arbetet har skett genom digitala arbetsgruppsmöten och eget arbete mellan dessa. Arbetsgruppen har träffats digitalt vid tio tillfällen. Samtliga enhetschefer vid SU har intervjuats under maj respektive juni.

Chefen för SÅK, överåklagare Anders Jakobsson, beslutade på förfrågan från chefen SU att utse chefsåklagaren Henrik Rasmusson som referensperson från SÅK. Per Blomqvist har haft tre avstämningsmöten med Henrik Rasmusson.

4 Resultat

4.1 Genomgång av nuläget

Brottet dataintrång anges i Brottsbalken 4 kap 9 c §.

”Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.”

Vid Polismyndigheten genomförs ett stort antal registerslagningar varje dygn. Den absoluta merparten av dessa görs inom ramen för de regelverk som styr polisens personuppgiftsbehandling. Dock sker även slagningar i polisiära system och andra system som polisen har tillgång till, utan att det är nödvändigt för att genomföra en viss arbetsuppgift. Att olovligt bereda sig tillgång till sådan uppgift innebär dataintrång. Det är Polismyndigheten som sätter ramarna för vad som är ett *olovligt* beredande till uppgift. Det har myndigheten bland annat gjort genom styrdokumentet *Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it PM 2017:4* (Se vidare under avsnitt 4.1.3 *Befogenhet och styrdokument*).

Problembilden för Polismyndigheten är bland annat att teknikutvecklingen är så snabb att den är svår att hinna möta med information och utbildning för regelefterlevnad. Generellt verkar också gemene man ha vant sig vid att snabbt kunna söka information via

Google och andra liknande system. Det finns risk att detta användarbeteende och syn på informationsinhämtning appliceras på polisens system. Nyligen tog till exempel medarbetare del av filmmaterial från kameraplattformen, sannolikt utan att reflektera över att detta är att *”bereda sig tillgång till uppgift som är avsedd för automatisk behandling”*. För Polismyndigheten är det också viktigt att skydda medborgarna från olovliga slagningar och att upprätthålla ett stort förtroende för myndighetens hantering av personuppgifter.

Problembilden för SU är svårigheten att utreda brotten. Främst beror det på bristen på tydlighet från myndigheten om vad som är otillåtna slagningar. Genom brister i utbildning blir det inte sällan oklart vad gäller uppsåtet. Områden som återkommer gång på gång i samband med misstanke om brott är vad som har varit arbetsuppgiften, vad som ingår i serviceskyldigheten och var gränsen för jäv går. Dataintrången kan kategoriseras i två huvudtyper av slagningar, anhörigslagningar/nyfikenhetsslagningar och mer systematiska och omfattande slagningar där det inte sällan finns misstanke om att uppgifter lämnats vidare till obehörig.

Arbetsgruppen identifierade tidigt åtta områden av särskilt intresse för det fortsatta arbetet. Dessa områden var följande:

- Domar.
- Nedläggningsgrunder.
- Befogenhet och styrdokument.
- Utbildning i informationssäkerhet.
- CSL.
- PAN (synen på brottsvolym i förhållande till arbetsrättsliga beslut).
- Brott mot tystnadsplikt (brott mot tystnadsplikt i kombination med dataintrång).
- Befintliga metodstöd inom ramen för PNU.

De utvalda områdena har på olika sätt koppling till effektmålet om en ensad och effektiviserad utredningsprocess samt ovan beskrivna nuläges- och problembild. Kartläggningen av befintliga metodstöd gjordes för att se om det var möjligt att återanvända delar av dessa i ett avdelningsgemensamt och enhetligt metodstöd.

4.1.1 Domar

Ett antal domar om dataintrång har genomgåts.³ Ämnen som återkommer i domarna utifrån uppsåtsfrågan är jäv, serviceskyldigheten, utbildning och information och vad som ingår i arbetsuppgiften. Olika motiveringar till varför man slagit i system som framkommit i domarna är att man inte hade vetskap om att man inte fick slå på vissa uppgifter i datorn, att man gjorde det för att man trodde att det ingick i arbetsuppgiften, att man gjorde det för att serva andra kollegor med information om vad som hänt i en viss utredning, av nyfikenhet, samt att man gjorde det för att man uppfattade att det ingick i serviceskyldigheten inom ramen för polisens arbete gentemot allmänhet och kollegor.

³ Se bilaga 2

4.1.2 Nedläggningsgrunder

Samtliga till SU inkomna ärenden under 2020 med brottskod 0415 (dataintrång) samt 9466 (dataintrång genom olovlig registerslagning) har genomgått⁴. Främsta anledningarna till upprättande av ärenden om dataintrång var slagningar på otillåten krets av personer (jäv) eller för slagning åt annan på otillåten krets. Totalt har 139 ärenden anmälts. Av dessa var förundersökning ej inledd för 41, 16 var pågående, 30 var nedlagda, 50 var redovisade till åklagare, ett var avställt och ett var återsänt till Polismyndigheten. Orsaker till nedläggning var bland annat bevisproblem, uppsåtsproblematik, att de påstådda slagningarna ej var gjorda (vid kontroll) samt att slagningarna varit nödvändiga för arbetsuppgiften. Inom bevis- och uppsåtsproblematiken ryms de ärenden där medarbetare inväntat att de varit i tron att de varit behöriga att göra slagningar, exempelvis genom att det förelegat en uppfattning om serviceskyldighet.

4.1.3 Befogenhet och styrdokument

Det viktigaste styrdokumentet inom området it-säkerhet är *Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it PM 2017:4*. I punkten 7.1.1 anges: *"It-system som är tillgängliga inom Polismyndigheten får användas endast när det är nödvändigt för att genomföra en viss arbetsuppgift. Det ska vara sannolikt att användandet i det enskilda fallet är till nytta för arbetets genomförande."* Dock utvecklas inte texten ytterligare vilket lämnar utrymme för egna tolkningar. Därför skulle texten behöva exemplifieras för att tydliggöra gränsen mellan tillåten och otillåten användning. Därtill kan arbetsgruppen se att riktlinjerna inte verkar vara tillräckligt implementerade inom Polismyndigheten.

4.1.4 Utbildning i informationssäkerhet

Polismyndigheten tillhandahåller en stor mängd utbildningar inom it-området. Flera av dessa är obligatoriska för att få viss behörighet. *Introduktionsutbildning i informationssäkerhet* är en utbildning i fem avsnitt i utbildningsportalen Ping Pong på Intrapolis. Genomgången utbildning med godkänt kunskapstest är obligatoriskt för att få tillgång till Polisens it-system. *Introduktionsutbildning i dataskydd* (DSU-intro) är en 15 minuter lång utbildning på Intrapolis som även den avslutas med ett kunskapsprov. Utbildningarna behandlar regelverk och myndighetens ansvar och vikten av att skydda informationen i systemen. Enskilda medarbetares ansvar presenteras dock på ett sätt som gör det lätt att uppfatta det som allmänna förhållningsregler. Utbildningarna behandlar inte särskilt otillåtna slagningar i system utan detta nämns bland andra punkter, såsom att rensa e-postlåda och att formulera sig korrekt i skrift. Kunskapstesterna har mycket lågt ställda krav.

I utbildningen för att få mobilt tjänste-id⁵ tydliggörs kraven i en knappt fyra min lång textad informationsfilm. Där definieras bland annat när det är tillåtet att göra slagningar utanför arbetstid. Där anges bland annat. *"mPMF⁶ får användas när man är i tjänst enligt de regler som vi omfattas av. Tjänsteutövning utanför arbetstid får endast ske i enlighet med 16§ i polisförordningen. All informationssökning som inte är tjänsterelate-*

⁴ Se bilaga 3

⁵ Mobilt tjänste-id är en förutsättning för att på ett förenklat sätt (utan engångskod från Pap eller Rakelstation) för att nå bland annat mPMF.

⁶ Polisens mobila multifråga som ger tillgång till ett antal IT-system via tjänstetelefonen dygnet runt.

rad eller görs utan att du har befogenhet kan vara att anses som dataintrång. Du får exempelvis inte göra slagningar på dig själv eller andra av ren nyfikenhet. Din slagning måste ha ett tydligt syfte som även ska kunna motiveras om så behövs och att tjänsteverktygen är till för tjänsten, i tjänsten.” Den utbildningen saknar ett kunskapstest.

Arbetsgruppen har inte i någon av utbildningarna, mer än ovan, funnit förtydligande var gränserna för bland annat befogenhet, serviceskyldighet och jäv går. Dessa gränser är av stor betydelse att tydliggöra för att kunna konstatera huruvida det funnits ett uppsåt att begå ett dataintrång. Det är även lätt att få uppfattningen att de berörda processägarna (NOA, it-, och HR-avdelningen) inte fullt ut har koordinerat sig i framtagandet av it-utbildningar. Dessutom saknas en sammanställning över enskildas genomgångna utbildningar och kunskapsprov. Dessa får vid behov sökas på olika ställen.

4.1.5 CSL

CSL är en sammanställning av aktivitetsloggning från ett stort antal olika system (fler än 80) innehållande olika information som levereras i olika format. CSL innehåller mycket relevant och användbar information för att kunna analysera, förstå och visualisera en användares aktiviteter i polisära it-system. De större brister som finns i aktivitetsloggningen inom Polismyndigheten beror på avsaknad av eller bristande loggning i enskilda källsystem, inte på CSL som sådan.

Då CSL i regel innehåller stora datamängder och informationen till stor del är av teknisk natur, krävs det vissa kompetenser för att på ett effektivt sätt och med hög kvalitet kunna bearbeta och tolka dess innehåll:

- Grundläggande förståelse för hur it-system är uppbyggda och fungerar (på en generell nivå).
- Kunskap om de polisiära system som omfattas av CSL, i form av användningsområden, informationsinnehåll etc.
- Kompetens inom kvantitativ analys, det vill säga förmågan att bearbeta stora datamängder och effektivt omvandla dessa till konkret och lättförståelig information.

4.1.6 PAN

I dialog med föredragande i PAN återger denna PAN:s inställning till brott rörande dataintrång kopplat till den arbetsrättsliga processen. Ju fler dataintrång som finns att bedöma, desto mer relevant arbetsrättsligt utlåtande kan PAN generera. Vilka register den enskilde har varit inne i vid brottstillfället är även det relevant. En större tyngd läggs på de register som har starkare skydd. En otillåten slagning i Allmänna spaningsregistret, ASP, är således att betrakta som allvarligare än en otillåten slagning i passsystemet RES. Kan det påvisas relationer, att den misstänkte fått vinning eller att informationen som extraherats har använts för att dela med annan, ser arbetsgivaren allvarligare på dataintrånget. Likaså bedöms ett repetitivt beteende allvarligare än enstaka dataintrång.

Ur ett arbetsrättsligt perspektiv kan det därmed föreligga en risk i att begränsa antalet slagningar inom förundersökningen. PAN ska kunna ges möjlighet att göra en adekvat bedömning baserat på antalet slagningar. Det kan föreligga skäl att analysera en större mängd data för att se om det finns en systematik i dataintrången hos den enskilde. Vi-

Dokument
RAPPORTSida
10 (16)

Upprättad av

Datum
2021-09-07Diariernr
A094.823/2021Saknr
129Version
01.01

dare bör en analys göras för att styrka en eventuell relation till föremålet för slagningarna. Sett ur detta perspektiv bör fråga rörande tidseffektivitet kontra uppdraget lagföring ställas mot varandra.

4.1.7 *Brott mot tystnadsplikt*

Arbetsgruppen har noterat att få ärenden om dataintrång också innehåller brott mot tystnadsplikt. I PM 2021-04-01 *Underlag - grovt brott mot tystnadsplikt* anges att den låga straffskalan för tystnadsplikt leder till att brottet blir svårt att styrka då ett styrkande normalt kräver avlyssning eller bevis i form av SMS-konversationer eller liknande. På grund av att det saknas möjlighet till vissa hemliga tvångsmedel saknas ofta stödbevisning avseende brott mot tystnadsplikt. I samma PM anges att det i de fall brott mot tystnadsplikt begås av en polisanställd inte är ovanligt att det föregås av ett dataintrång, där den polisanställda sedan röjer uppgiften som han eller hon olovligen berett sig tillgång till. Ofta utreds inte brott mot tystnadsplikt i dessa fall mot bakgrund av att det inte finns anledning att vidta omfattande utredningsåtgärder när brott mot tystnadsplikt inte påverkar straffet och utredningarna ofta är komplicerade.

4.1.8 *Metodstöd, PNU, med mera*

Befintliga tre metodstöd vid Polismyndigheten är *Dataintrång genom olovlig registerslagning, brottskod 9466*, *Dataintrång i sociala medier eller e-tjänster, brottskod 9467* samt *Övrigt dataintrång, brottskod 9468*. Samtliga från 2020-07-01. Dessa är av begränsad nytta för SU:s utredningar då de berör externa dataintrång med andra frågor än de som berör SU:s utredningar.

4.2 *Beskrivning och analys av den befintliga processen*⁷

Misstankar om dataintrång når vanligen SU antingen genom SU:s egen underrättelseverksamhet, framför allt genom olika CSL-kontroller, eller genom att en kollega eller annan anmäler att en polisanställd har kännedom om något som hen inte borde. Det förekommer även att ärenden initieras i samband med att nya misstankar uppdagas vid en redan pågående brottsutredning.

När ärendet inkommer kontrollerar ärendesamordningen först uppgifterna för att kvalitetssäkra dem. Vid behov hämtas därefter kompletterande underlag in. Ju fullständigare det som inkommer från början är, desto snabbare går arbetet för ärendesamordningen. Då underlaget kommer från underrättelseenheten vid SU upprättas ett *Underlag för anmälan om dataintrång*⁸. Underrättelseenheten tar ibland i samband med detta fram andra underlag, såsom till exempel den berördes arbetstider, vilket underlättar samordnarens arbete.

Det är ärendesamordningen som upprättar anmälan och lottar ärendet till SÅK. I de fall en åklagare beslutar att en förundersökning ska inledas, lägger samordnaren över ärendet på en utredningsenhet.

Åklagarens direktiv styr hur utredningen ska bedrivas. Samarbetet mellan utredaren och åklagaren fungerar oftast mycket bra, men är hög grad personberoende och det saknas

⁷ Se bilaga 4

⁸ Se bilaga 5. Underlaget används för närvarande inte.

enhetliga arbetssätt. Antalsräkningen är ett exempel där arbetssätten varierar, vilket i sin tur påverkar strukturen på utredningsarbetet. Olika arbetssätt, till exempel att varje utredare tar fram egna mallar och checklistor, innebär även risk för dubbelarbete och skiftande kvalitet.

När tillräckligt med bevis har inhämtats, sammanställs redovisningen och överlämnas till åklagaren för beslut. Processen avslutas med att åklagaren fattar beslut om huruvida åtal ska väckas eller inte. Om åklagaren fattar beslut om nytt direktiv börjar processen om på nytt.

Nedan beskrivs hinder respektive framgångsfaktorer i samband utredningsprocessen mer ingående.

4.2.1 Befintliga och framtida hinder och framgångsfaktorer

Ett av målen i uppdraget har varit att identifiera befintliga och framtida framgångsfaktorer respektive hinder för att effektivisera utredningsprocessen vid dataintrång. Två seminarier har därför genomförts i arbetsgruppen för att hitta dessa faktorer. Hindren bedömdes utifrån konsekvensernas storlek och framgångsfaktorerna på motsvarande sätt utifrån nyttan. Slutligen gjordes vid seminarierna en bedömning av huruvida hindren och framgångsfaktorerna befinner sig inom eller utom SU:s kontroll, för att på så sätt identifiera adekvata åtgärder. Med inom SU:s kontroll avses det som SU av egen kraft och mandat kan råda över, medan det motsatta gäller för det som har bedömts vara utom SU:s kontroll.

Hinder och framgångsfaktorer har dokumenterats dels i tabellform, dels i en bedömningsmall⁹. Sammanfattningsvis kan sägas att många hinder har bedömts ligga utanför SU:s kontroll. Det handlar till exempel om de brister i utbildning och behörighetshantering samt den otydlighet kring vilka slagningar man får göra inom ramen för sitt uppdrag, som redan har tagits upp ovan. Att hinder ligger utom SU:s kontroll innebär inte per automatik att de inte går att påverka. Under avsnitt 4.4 *Förslag till åtgärder inom övriga Polismyndigheten* förs ett närmare resonemang om detta.

Avsaknad av ett gemensamt metodstöd samt kompetensbrister är exempel på två hinder som har bedömts ligga inom SU:s kontroll. Frånvaron av ett gemensamt metodstöd är kanske det hinder som enklast kan omvandlas till framgångsfaktor. Med ett samlat metodstöd kan tidsbesparingar göras genom att den enskilda utredaren slipper leta eller ta fram saker på egen hand. När alla gör mer lika, exempelvis med hjälp av mallar och checklistor, uppstår även kvalitetsvinster. Samtidigt underlättas åklagarnas arbete när utredning och redovisning blir mer enhetlig. På så sätt kan hela processen effektiviseras. Dock behöver det finnas utrymme att göra avsteg i de fall det behövs, eftersom utredningarnas omfattning, karaktär och komplexitet i hög grad varierar. Vad ett gemensamt metodstöd föreslås innehålla mer konkret finns beskrivet under avsnitt 4.3.2 *Gemensamt metodstöd*.

⁹ Se bilagorna 6-1, 6-2, 7-1 och 7-2.

Även hindret ”brist på analytisk förmåga” skulle genom kompetenshöjning kunna omvandlas till en framgångsfaktor. Ytterligare en potentiell framgångsfaktor är programvaran Excel. Rätt använd är Excel ett bra analysstöd med bland annat goda filtreringsmöjligheter att hantera stora datamängder. Arbetsgruppens bedömning är att en ökad förmåga inom detta område skulle kunna bidra till att effektivisera utredningsarbetet. Under avsnitt 4.3.1 *Kompetenshöjning inom SU* redogörs närmare för vilka brister som arbetsgruppen ser och vilka åtgärder som föreslås inom detta område.

När det gäller befintliga framgångsfaktorer har merparten bedömts ligga inom SU:s kontroll. Ett exempel är underrättelseenhetens underlag till utredningssidan. Visserligen finns det förbättringsmöjligheter, men redan idag är de en framgångsfaktor. Ett annat exempel är korta beslutsvägar, där SU tillsammans med SÅK äger processen och därmed också möjligheten att komma överens om ett samlat och enhetligt metodstöd och gemensamma modeller för utredning och uppföljning.

Ett exempel på en befintlig och samtidigt möjlig framtida framgångsfaktor utom SU:s kontroll, åtminstone delvis, är loggningen av it-systemen. Beskrivningar av CSL och dess centrala roll vid dataintrången återkommer på flera ställen i rapporten och tas därför inte upp närmare här.

4.3 Förslag till åtgärder

Med de erfarenheter arbetsgruppen dragit samt hur direktivet är utformat föreslår arbetsgruppen nedan åtgärder. En del av åtgärderna vänder sig till övriga delar av myndigheten. Detta ingick inte i direktivet, men arbetsgruppen anser att åtgärderna är så viktiga att de ändå behöver finnas med i rapporten. Dessa förslag till åtgärder återfinns under avsnitt 4.4 *Förslag till åtgärder inom övriga Polismyndigheten*.

4.3.1 Kompetenshöjning inom SU

Det är viktigt att avdelningen har rätt kompetens för att effektivt kunna utreda dataintrång. Dels behövs en allmän kunskap vid berörda enheter om hur processen ser ut i sin helhet, så att var och en vidtar rätt åtgärder för att underlätta för nästa steg i utredningen, dels behövs kompetens vid utredningsenheterna både för att utreda dataintrång av normalgraden liksom för de större utredningar som inkommer. Det behöver säkerställas en lägsta kompetens vid utredningsenheterna för att a/ kunna behandla större datamängder i Excel, och b/ kunna läsa CSL-underlag. Då analysförmågan är en trång sektor vid utredningsenheterna behövs en ökad analytisk förmåga där. Förslag till kompetenshöjande åtgärder är:

- Ett gemensamt seminarium med SÅK under den gemensamma konferensen november 2021.
- En inventering av kunskaperna i Excel för utredarna och kompetenshöjande åtgärder för dem som behöver det.
- Ett seminarium om CSL med utredare vid enheterna, handläggare vid underrättelseenheten och medarbetare vid CSL.
- Att SU överväger att öka den analytiska förmågan vid SU:s utredande verksamhet.
- Ökad kunskap i CSL (att tolka innehållet) för utredarna.
- En enklare e-utbildning om dataintrång för nya utredare vid SU som kan tas fram till exempel genom en Powerpointpresentation.

- Allmän kunskap i Durtvå plus, för att kunna använda mallar som anges under avsnitt 4.3.5 *Samarbete med SÅK*.

4.3.2 *Gemensamt metodstöd*

Ett avdelningsgemensamt metodstöd behöver färdigställas och beslutas i samarbete med SÅK. Innehållet ska underlätta ett standardiserat arbetsflöde och innehålla checklistor för att tydliggöra ansvarsfördelning, undvika dubbelarbete och underlätta strukturering av förundersökningsprotokoll, olika arbetsmoment, med mera. Bland annat behöver det framgå vilka underlag som har tagits fram i ett tidigt skede, för att inte behöva ta fram dessa underlag vid ytterligare tillfällen. På sikt kan mallar finnas i Durtvå plus. (Det kräver dock en allmän kunskap i denna version av Durtvå.)

Grunden till ett gemensamt metodstöd har tagits fram av arbetsgruppen. Det består av insamlat material som har sparats ner på I: i ett mappsysteem som har följande huvudkataloger:

1. *Metodstöd (inklusive checklistor, lathundar, etc.)*

Här ska stödmaterialet för utredningsarbetet finnas, såsom mallar, checklistor, med mera.

2. *Regelverk och styrdokument*

Denna mapp ska innehålla både befintliga och tidigare styrdokument, med angivelse för vilken tidsrymd dokumenten gällde. Detta för att kunna se vad som gällde vid en viss tidpunkt.

3. *It-system A-Ö (inklusive varningstexter)*

Denna mapp ska innehålla en standardiserad beskrivning av samtliga it-system som har tagits fram av respektive informationsägare. Information som ingår i förundersökningsprotokollet. Mappen ska även innehålla de skärmbilder som visas i samband med inloggning, etc. samt under vilken tidsrymd varningstexterna var aktuella.

4. *Utbildning*

Mappen ska innehålla information om relevanta utbildningar och användarstöd. Ibland hela innehållet nedladdat samt daterat för att kunna användas vid misstanke om dataintrång som härrör sig tillbaka i tiden.

5. *Logg, visualisering, presentation*

I denna mapp ska olika visualiseringar sparas.

6. *Rättspraxis och rättsutredningar*

Denna mapp ska innehålla domar, rättsliga kommentarer, rättsutredningar, m.m.

7. *Övrigt*

Mappen ska innehålla relevant material som inte ska sparas i någon av de övriga mapparna.

Varje mapp innehåller ett dokument om heter *Läs mig först*. Det dokumentet innehåller en förklarande text över mappinnehållet samt vem som ansvarar för innehållet och när det uppdaterades senast. Förslagsvis delas ansvaret mellan enheterna.

4.3.3 *Mall från underrättelseenheten*

Den befintliga *Underlag för anmälan om dataintrång(bil 3)* som har tagits fram under våren 2021 används för närvarande inte då den är under revidering. Arbetsgruppen bedömer att det underlaget kan utvecklas ytterligare. Detta kan ske vid det seminarium som föreslås nedan. Det behöver även tydliggöras vilken information underrättelseen-

heten kan lämna till förundersökningen i respektive ärende och därmed värdera ärendets känslighet ur ett underrättelseperspektiv.

4.3.4 Modell för återkoppling

SU:s enheter bör gemensamt med SÅK ha ett årligt seminarium som handlar om dataintrång. Seminariet förbereds av en arbetsgrupp som träffas kontinuerligt. Lämpliga ämnen för seminariet är hinder, framgångsfaktorer, nyheter (regelverk, teknik, metod respektive beteende) samt eventuella behov av förändringar.

Återkoppling i specifika utredningar hela vägen bör ske dels genom kontakt mellan enskilda, i bägge riktningar, det vill säga en utredare vid utredningsenheterna återkopplar bakåt vad som varit framgångsfaktorer resp. hinder i en speciell utredning, liksom att utredare vid samordningen resp. underrättelsehandläggare söker information om ärendens vidare handläggning vid utredningsenheterna. Efter det att större ärenden utretts ansvarar berörda enhetschefer för att samla involverade medarbetare för gemensam genomgång av ärendet.

Egen återkoppling i det enskilda fallet sker löpande genom att utredare och underrättelsehandläggare tar del av domar och nedläggningsbeslut i ärenden som man varit delaktig i.

4.3.5 Samarbete med SÅK

SU och SÅK bör ta fram en gemensam grundmall för förundersökningar som berör dataintrång. Mallen, som lämpligen på sikt byggs i Durtvå plus, innehåller generella direktiv och en gemensam disposition. (När samtlig utredande personal har erforderlig utbildning och vana i att utreda i Durtvå Plus) Till mallen finns kompletterande material i gemensam mapp på I, som innehåller den systemspecifika information som anges under avsnitt 4.3.2 *Gemensamt metodstöd*.

En gemensam syn på antalsräkning avseende brott behöver överenskommas mellan SU och SÅK eftersom sådan saknas i nuläget. Genomgång av ärenden som inkommit under år 2020 har visat att redovisning av brott sker på olika sätt i utredningarna. I överenskommelse mellan Särskilda åklagarkammaren och avdelningen för särskilda utredningar om handläggningen av ärenden med mera(daterad 2021-01-08) under punkten 5.4 "Särskilt om dataintrång" nämns att "om polisanställd gjort fler än tio otillåtna slagningar ska SU kontakta SÅK för samsyn om vidare hantering." I dessa fall kan lämpligen ett brott gällande dataintrång med brottstid som täcker alla slagningar läggas upp initialt. Därefter bör kontakt tas med ansvarig åklagare innan ett brott eventuellt läggs upp för varje slagning. Detta för att undvika merarbetet att lägga upp brott i de fall där utredningen inte leder vidare eller där åklagaren har en annan syn på antalsberäkningen. När det rör sig om mycket stora mängder slagningar (över 100) behöver ett brott per slagning inte heller läggas upp enligt RIF.

Arbetsgruppens förslag är att brotten om möjligt registreras i ett tidigt skede i Durtvå. Dock med hänsyn till de beslut och överenskommelser som finns inom området och det som nämns ovan. Genom detta kan en god struktur skapas i utredningsskedet då slagningar ofta ska kopplas till handlingar/ dokument som inhämtats i ärendet avseende de enskilda brotten som skett vid olika tillfällen. En struktur kan då skapas för de enskilda brotten inför ett förundersökningsprotokoll i ärendet. Även beslut avseende enskilda

Dokument
RAPPORTSida
15 (16)

Upprättad av

Datum
2021-09-07Diariennr
A094.823/2021Saknr
129Version
01.01

brott kan genom detta spåras (exempelvis förundersökningsbegränsning eller bevisproblematik i det enskilda brottet)

4.3.6 Särskilt om CSL

Som nämnts under avsnitt 4.1.5 *CSL*, krävs en del specifika kompetenser för att på ett effektivt och kvalitetssäkrat sätt kunna bearbeta och tolka *CSL*. För att förenkla detta arbete och möjliggöra att så många som möjligt uppfyller nödvändiga kompetenskrav bör standardiserade riktlinjer, mallar och rutiner tas fram för bearbetning, tolkning och presentation av *CSL*. Därtill behövs ett fortsatt samarbete mellan SU underrättelseenhet och *CSL* i syfte att ytterligare förfinas möjligheterna att hitta olovliga slagningar. I det sammanhanget kan även nämnas att arbetsgruppen ser att *CSL* borde ha en större redundans med tanke på verksamhetens vikt för att upptäcka otillåtna slagningar.

4.4 Förslag till åtgärder inom övriga Polismyndigheten

I direktivet framgår det inte att arbetsgruppen ska föreslå åtgärder som berör övriga Polismyndigheten. Under arbetet har det dock framgått att ett antal viktiga åtgärder från andra delar av myndigheten är av stor betydelse både för det utredande liksom det förebyggande arbetet kring dataintrång. Därför presenterar arbetsgruppen nedan beskrivna förslag till åtgärder.

Det är angeläget att ett sådant samarbetsforum som beskrivs under avsnitt 2.4 *Tidigare arbete* (it-avdelningen, Säkerhetssavdelningen, SU, och berörda informationsägare) etableras för att hantera många av de frågor som är avdelningsgemensamma och anges i denna rapport.

Myndighetens it-säkerhetsutbildningar har brister. Därför behöver hela it-säkerhetsutbildningsområdet ses över. Ett system för obligatorisk utbildning i it-säkerhet med återkommande repetition behöver införas. Myndigheten behöver samla bevis på genomgången utbildning på ett ställe, lämpligen PAP. I it-säkerhetsutbildningarna behövs ett tydliggörande vad gäller befogenhet, serviceskyldighet och jäv göras med exemplifieringar. Särskilt behövs utbildning för nyanställda och polisstudenter så att de förstår skillnaden mellan att slå i polisiära system och att *Googla*. Utbildningen/informationen behöver klargöra att uppgifternas eventuella sekretess eller känslighet inte påverkar lovligheten att bereda sig tillgång till dem.

Polismyndigheten bör använda möjligheten att genomföra systematiska brottsförebyggande kampanjer inom myndigheten, speciellt i samband med nya tekniska lanseringar, såsom exempelvis kameraplattformen, för att tydliggöra regelverket i samband med ökad tillgänglighet av information.

Myndigheten behöver se över behörigheterna till olika system i syfte att endast de som har behov har behörighet.

Varje informationsägare behöver i samråd med SU ta fram ett underlag med beskrivning av systemet, vad som framkommer vid respektive slagning i systemet, skärmdumpar utvisande hur systemet ser ut och vilka val som kan göras vid slagningar, med mera. Materialet ska kunna användas motsvarande som en "Lathund för dummys" och utgöra en beskrivning som kan redovisas i domstol samt kontaktmöjlighet för kompletterade

frågor från SÅK. På motsvarande sätt behöver också systembeskrivningar för externa system som exempelvis systemen PIL, KVR och VTR tas fram.

Myndigheten behöver tydliggöra gränsen mellan lovligt och olovligt användande av it-system i styrdokument och utbildningar. I de fall där det är möjligt, behöver gränsen exemplifieras.

I samband med införande av ny teknik respektive funktionalitet behöver myndigheten bedöma behov av utbildning samt information. I samband med sådan information behöver upptäcktsrisken och konsekvenserna påtalas.

Det behöver göras ändring i tjänstetelefonerna så att platsinfo ej kan slås av vid slagning i polisiära system.

5 Förslag till fortsatt arbete

För att resultat ska nås behöver följande åtgärder vidtas.¹⁰

5.1 Utbildning

Inventera det interna utbildningsbehovet som beskrivs under avsnitt 4.3.1 *Kompetenshöjning inom SU* och planera och genomföra utbildningen, samt ta fram den beskrivna e-utbildningen.

Planera och genomföra de angivna seminarierna med SÅK respektive CSL.

5.2 Metodstöd

Bilda en gemensam arbetsgrupp mellan SU och SÅK för att med det insamlade materialet som grund ta fram ett gemensamt metodstöd och en grundmall för förundersökningsprotokoll där grundmallen är prioriterad. Genom att använda arbetsgruppens deltagare från utredningsenheterna tillsammans med referenspersonen från SÅK, tappas inte tempo i frågan. Genom att adjungera arbetsgruppens deltagare från underrättelseenheten kan arbetet även innefatta en uppdatering av UND-mallen. Ta fram en ansvarsfördelning för att förvalta det framtagna metodstödet.

5.3 Modell för återkoppling

Ge SU kansli i uppdrag att ansvara för att modellen för återkoppling genomförs.

5.4 Övriga åtgärder

Ge SU kansli i uppdrag att söka förmå it-avdelningen att initiera det samarbetsforum som anges under avsnitt 2.4 *Tidigare arbete* för att därigenom hantera de förslag till åtgärder som anges under avsnitt 4.4. *Förslag till åtgärder inom övriga Polismyndigheten*.

¹⁰ Åtgärderna sammanställs i bilaga 8.



PM

Utbildning

Signerad av

Signerad datum

Enhet

Särskilda utredningar, Utredning 1 Göteborg SU

Diarienumr

0150-K2050-20

Uppgiftslämnare

Edsand, Mats

Datum

2021-12-13

Tid

10:14

Beslag verkställt

Nej

Material för analys

Nej

Mottaget

Mottaget datum

Tid

Sätt på vilket uppgift lämnats

Upprättad av

Mats Edsand

Involverade personer

Personnummer/Orgnr

Roll

Hjortmarker, Sarah

Annan

Uppgiften avser

Dokumentation om utbildning för Martin Ambjörnsson

Uppgift

Handläggare kontaktar Sarah Hjortmarker, chef för mobilitet, för att klargöra hur utbildningen går till för att få en telefon innehållande applikationerna för att göra slagningar i polisen system.

Hjortmarker uppger att man måste ha genomgått en utbildning. för att få en mobil. I början hade man klassrumsutbildning, för de 10 000 st första, för att sedan övergå till digital utbildning. Vid klassrumsutbildning så skrev läraren ned vilka som hade genomgått utbildningen. därefter skickade lärarna listan till dem och de gav dem behörigheten. Klassrumsutbildningen påbörjades våren 2016 med 2000 st i månaden. Man får inte en telefon utan att genomgått utbildningen. Detta var ett starkt krav från facket med att alla skulle genomgå utbildningen innan de fick mobiltelefonens applikationer.

Hjortmarker förklarar att under 2016 gjordes det klassrumsutbildningar, dessa var på 2-4 timmar. När de var klara så skrev läraren upp allas U-nr som skickades in centralt för att få tillgång till polisens applikationer. Sedan fick man gå en Info och säkerhetsutbildning som visade att man hade förstått. Därefter är man tvungen att skaffa ett Tjänste ID för att kunna starta applikationen.

2017 övergick klassrumsutbildningen till Ping-Pong utbildning, d.v.s. via nätet.

Sarah Hjortmarker fick U-numret på den aktuella polismannen för att se om de hade någon registrering.

U0027303 kontrollerades av Hjortmarker. Hennes uppgifter visar att polismannen gick klassrumsundervisning som registrerades v. 51 år 2016. Det finns inget utbildningsbevis på detta.

Har personen varit i tjänst sedan dess så har personen också genomgått

TjänsteID-utbildningen. Har han yttre tjänst så tror Hjortmarker att han gjort den i mobilen.

Då har personen kryssat i att "ja jag förstår att jag inte skall jobba dygnet runt. Ja jag förstår att mPMF skall användas för tjänsten".

Det går alldeles utmärkt att genomgå utbildningen igen som kan registreras detta datum.

Skapad 20211208:0930

Persons tjänstgöring Översikt: 20190624-20190831/MARAMB/S/830922-6234/Ambjörnsson Martin

Organhet	Datum	Dag	Funktion	Fa f	Fa t	Rast	Nettotid	A1
550430IG3	20190624	Må	OMRPOL	06:45	16:30	0:0	09:45	
550430IG3	20190625	Ti	OMRPOL	06:45	16:30	0:0	09:45	
550430IG3	20190626	On	OMRPOL	06:45	18:15	0:0	11:30	ÖT
	20190627	To		F		0:0		
	20190628	Fr		SF		0:0		
	20190629	Lö		SF		0:0		
	20190630	Sö		SF		0:0		
550430IG3	20190701	Må	OMRPOL	14:30	23:00	0:0	08:30	
550430IG3	20190702	Ti	OMRPOL	10:00	18:30	0:0	08:30	
	20190703	On		F		0:0		
	20190704	To		F		0:0		
550430IG1	20190705	Fr	INGRIPOL	15:00	24:00	0:0	09:00	
	20190706	Lö	GRPMEDL	18:00	03:00	0:0	09:00	TF
550430IG3	20190706	Lö	OMRPOL	03:00	03:45	0:0	00:45	TF
	20190707	Sö				0:0		
	20190708	Må		F		0:0		
550430IG3	20190709	Ti	OMRPOL	14:30	23:00	0:0	08:30	
550430IG3	20190710	On	OMRPOL	14:30	00:05	0:0	09:35	ÖT
	20190711	To		-		0:0		
	20190712	Fr		17:00	03:00	0:0	10:00	TF
	20190713	Lö		17:00	03:00	0:0	10:00	ÖT
	20190714	Sö				0:0		
550430IG3	20190715	Må	OMRPOL	06:45	16:30	0:0	09:45	
550430IG3	20190716	Ti	OMRPOL	06:45	16:30	0:0	09:45	
550430IG3	20190717	On	OMRPOL	06:45	16:30	0:0	09:45	
550430IG3	20190718	To	OMRPOL	06:45	16:30	0:0	09:45	
	20190719	Fr		SF		0:0		
	20190720	Lö		SF		0:0		

	20190721	Sö		SF		0:0			
550430IG2	20190722	Må	INGRIPOL	14:30	23:00	0:0	08:30		
550430IG3	20190723	Ti	OMRPOL	10:00	18:30	0:0	08:30		
	20190724	On		F		0:0			
	20190725	To	GRPMEDL	17:00	03:00	0:0	10:00	ÖT	
550430IG3	20190725	To	OMRPOL	03:00	05:45	0:0	02:45	ÖT	
550430IG2	20190726	Fr	INGRIPOL	15:00	24:00	0:0	09:00		
	20190727	Lö		-		0:0			
550430IG2	20190728	Sö	INGRIPOL	06:45	16:30	0:0	09:45		
	20190729	Må		SF		0:0			
	20190730	Ti		F		0:0			
550430IG3	20190731	On	OMRPOL	14:30	24:00	0:0	09:30	ÖT	
	20190801	To		-		0:0			
	20190802	Fr				0:0			
	20190803	Lö				0:0			
	20190804	Sö				0:0			
	20190805	Må				0:0			
	20190806	Ti				0:0			
	20190807	On				0:0			
	20190808	To				0:0			
	20190809	Fr				0:0			
	20190810	Lö				0:0			
	20190811	Sö				0:0			
	20190812	Må				0:0			
	20190813	Ti				0:0			
	20190814	On				0:0			
	20190815	To				0:0			
	20190816	Fr				0:0			
	20190817	Lö				0:0			
	20190818	Sö				0:0			
	20190819	Må		F		0:0			
550430IG3	20190820	Ti	OMRPOL	14:30	23:00	0:0	08:30		

550430IG3	20190821	On	OMRPOL	14:30	23:00	0:0	08:30	
	20190822	To		-		0:0		
550430IG3	20190823	Fr	OMRPOL	10:00	18:30	0:0	08:30	
	20190824	Lö	F	F		0:0		
	20190825	Sö		F		0:0		
550430IG3	20190826	Må	OMRPOL	06:45	16:30	0:0	09:45	
	20190827	Ti	DELTA GAR	06:45	16:30	0:0	09:45	
550430IG3	20190828	On	OMRPOL	08:45	18:00	0:0	09:15	ÖT
550430IG3	20190829	To	OMRPOL	06:45	17:15	0:0	10:30	ÖT
	20190830	Fr		SF		0:0		
	20190831	Lö		SF		0:0		

Tjänstgöringstider från Cops på Martin Ambjörnsson

550430IG3 = BF - IGV 3 LPO S Fyrbodol

Skapad 20211208:0932

Personers tjänstgöring Översikt: 20191125-20200131/MARAMB/S/830922-6234/Ambjörnsson Martin

Orgenhet	Datum	Dag	Funktion	Fa f	Fa t	Rast	Nettotid	A1	A2	Fvk	Fvs	Fv f	Fv t	Fv Info
550430UT1	20191125	Må	UTREDARE	11:00	16:00	0:30	04:30			150		00:00	11:00	
550430UT1	20191126	Ti	UTREDARE	07:30	16:00	0:30	08:00							
	20191127	On				0:0				130		07:30	24:00	
	20191128	To				0:0				130		00:00	16:00	
	20191129	Fr				0:0				130		00:00	16:00	
	20191130	Lö		SF		0:0								
	20191201	Sö		SF		0:0								
550430UT1	20191202	Må	UTREDARE	07:30	16:00	0:30	08:00							
550430UT1	20191203	Ti	UTREDARE	07:30	16:00	0:30	08:00							
550430UT1	20191204	On	UTREDARE	11:00	16:00	0:30	04:30			150		07:30	11:00	
550430UT1	20191205	To	UTREDARE	07:30	16:00	0:30	08:00							
	20191206	Fr				0:0				130		07:30	16:00	
	20191207	Lö		F		0:0								
	20191208	Sö		F		0:0								
550430UT1	20191209	Må	UTREDARE	07:30	16:00	0:30	08:00							
	20191210	Ti	DELTAGAR	07:30	16:00	0:30	08:00							
550430UT1	20191211	On	UTREDARE	07:30	16:00	0:30	08:00							
550430UT1	20191212	To	UTREDARE	07:30	16:00	0:30	08:00							
550430UT1	20191213	Fr	UTREDARE	07:30	16:00	0:30	08:00							
	20191214	Lö		SF		0:0								
	20191215	Sö		SF		0:0								
550430UT1	20191216	Må	UTREDARE	07:30	16:00	0:30	08:00							
550430UT1	20191217	Ti	UTREDARE	07:30	16:00	0:30	08:00							
550430UT1	20191218	On	UTREDARE	08:30	16:00	0:30	07:00			150		07:30	08:30	
550430UT1	20191219	To	UTREDARE	08:30	16:00	0:30	07:00			150		07:30	08:30	
	20191220	Fr				0:0				130		07:30	16:00	
550430UT1	20191221	Lö	UTREDARE	12:30	13:00	0:0	00:30	ÖT						
	20191222	Sö		F		0:0								

	20191223	Må						0:0					130		07:30	24:00	
	20191224	Ti						0:0					130		00:00	24:00	
	20191225	On						0:0					130		00:00	24:00	
	20191226	To						0:0					130		00:00	16:00	
	20191227	Fr						0:0					130		00:00	16:00	
	20191228	Lö			SF			0:0									
	20191229	Sö			SF			0:0									
550430UT1	20191230	Må	UTREDARE	07:30	16:00	08:00		0:30									
	20191231	Ti		F				0:0									
	20200101	On						0:0					110		00:00	24:00	
	20200102	To						0:0					110		00:00	24:00	
	20200102	To						0:0					110		00:00	24:00	
	20200103	Fr						0:0					110		00:00	24:00	
	20200103	Fr						0:0					110		00:00	24:00	
	20200104	Lö						0:0					110		00:00	24:00	
	20200104	Lö						0:0					110		00:00	24:00	
	20200105	Sö						0:0					110		00:00	24:00	
	20200105	Sö						0:0					110		00:00	24:00	
	20200106	Må						0:0					110		00:00	24:00	
	20200106	Må						0:0					110		00:00	24:00	
	20200107	Ti						0:0					110		00:00	24:00	
	20200107	Ti						0:0					110		00:00	24:00	
	20200108	On						0:0					110		00:00	24:00	
	20200108	On						0:0					110		00:00	24:00	
	20200109	To						0:0					110		00:00	24:00	
	20200109	To						0:0					110		00:00	24:00	
	20200110	Fr						0:0					110		00:00	24:00	
	20200110	Fr						0:0					110		00:00	24:00	
	20200111	Lö						0:0					110		00:00	24:00	
	20200111	Lö						0:0					110		00:00	24:00	
	20200112	Sö						0:0					110		00:00	24:00	
	20200112	Sö						0:0					110		00:00	24:00	

20200113	Må							0:0						110	00:00	24:00	
20200113	Må							0:0						110	00:00	24:00	
20200114	Ti							0:0						110	00:00	24:00	
20200114	Ti							0:0						110	00:00	24:00	
20200115	On							0:0						110	00:00	24:00	
20200115	On							0:0						110	00:00	24:00	
20200116	To							0:0						110	00:00	24:00	
20200116	To							0:0						110	00:00	24:00	
20200117	Fr							0:0						110	00:00	24:00	
20200117	Fr							0:0						110	00:00	24:00	
20200118	Lö							0:0						110	00:00	24:00	
20200118	Lö							0:0						110	00:00	24:00	
20200119	Sö							0:0						110	00:00	24:00	
20200119	Sö							0:0						110	00:00	24:00	
20200120	Må							0:0						110	00:00	24:00	
20200120	Må							0:0						110	00:00	24:00	
20200121	Ti							0:0						110	00:00	24:00	
20200121	Ti							0:0						110	00:00	24:00	
20200122	On							0:0						110	00:00	24:00	
20200122	On							0:0						110	00:00	24:00	
20200123	To							0:0						110	00:00	24:00	
20200123	To							0:0						110	00:00	24:00	
20200124	Fr							0:0						110	00:00	24:00	
20200124	Fr							0:0						110	00:00	24:00	
20200125	Lö							0:0						110	00:00	24:00	
20200125	Lö							0:0						110	00:00	24:00	
20200126	Sö							0:0						110	00:00	24:00	
20200126	Sö							0:0						110	00:00	24:00	
20200127	Må							0:0						110	00:00	24:00	
20200127	Må							0:0						110	00:00	24:00	
20200128	Ti							0:0						110	00:00	24:00	
20200128	Ti							0:0						110	00:00	24:00	

	20200129	On						0:0				110	00:00	24:00	
	20200129	On						0:0				110	00:00	24:00	
	20200130	To						0:0				110	00:00	24:00	
	20200130	To						0:0				110	00:00	24:00	
	20200131	Fr						0:0				110	00:00	24:00	
	20200131	Fr						0:0				110	00:00	24:00	

Utdrag från Cops Tjänstgöringstider för Martin Ambjörnsson 2019-06-03 och 2019-12-06.
 Organisationsenhet 550430UT1 = Utredning 1 LPO S Fyrbodal



Polisen

36

PM

Frånvarokoder i Cops

Signerad av

Signerad datum

Enhet

Särskilda utredningar, Utredning 1 Göteborg SU

Diariet

0150-K2050-20

Uppgiftslämnare

Edsand, Mats

Datum

2021-12-22

Tid

09:25

Beslag verkställt

Nej

Material för analys

Nej

Mottaget

Mottaget datum

Tid

Sätt på vilket uppgift lämnats

Upprättad av

Mats Edsand

Uppgiften avser

Frånvarokoder i Cops

Uppgift

Frånvaro kod frånvarokodsbenämning

- | | |
|-----|---|
| 110 | Sjuk |
| 111 | SJUKBIDRAG/FÖRTIDSPENSION |
| 120 | Delpension |
| 130 | Uttag tim semester |
| 140 | FN-tjänst |
| 141 | TJL kommenderad (RPS,SÄPO,RKP,PHS) |
| 142 | Annan anställning/Tjänsteförening |
| 143 | Studier/ledighet med och utan lön |
| 144 | Tjänstledighet övrigt |
| 150 | Tillf. föräldrapenning - VAB och pappadagar"" |
| 151 | Föräldraled. med o. utan ersättning från FK |
| 160 | Kompensationsledighet (ÖT-komp/Mertid) |
| 161 | Uttag av Tidssaldo (Pass- eller tidsbyte) |
| 162 | Individuell tidskompensation |
| 163 | Flexitidskompensation (hel dag) |
| 164 | Kompleddighet för fullgjord veckoslutsberedskap |
| 170 | Läkarbesök |
| 171 | Nedkortning vid utebliven rast pga verksamhetsskä |
| 180 | Frånvaro inlånad |

I aktuellt ärende har Martin Ambjörnsson varit frånvaro med koden 110 från 2020-01-01 t.o.m. 2020-03-16. Då började Ambjörnsson som trafikpolis. Arbetar sedan en vecka för att på nytt ha frånvaro med koden 110 i tre dagar.



POLISVÄSENDET

SEKRETESSINFORMATION

Datum

2010-01-26

PERSONUPPGIFTER

Efternamn Ambjörnsson	Tilltalsnamn Martin	Personnummer 830922-6234
Tjänst Polisaspirant	Tjänsteställe Kungälv	
Postadress (utdelningsadress, postnummer och ortsadress) Ståleås Bygata 27 44254 Kungälv		

Jag har denna dag blivit informerad om de grundläggande bestämmelserna i tryckfrihetsförordningen och sekretesslagen (1980:100) samt om 1a § sekretessförordningen (1980:657). Jag har bl.a. upplysts om vad som menas med sekretess, vem som är skyldig att iaktta sekretessreglerna samt om bestämmelserna i 15 kap. sekretesslagen om lämnande av uppgift och utlämnande av allmän handling.

Därutöver har jag informerats särskilt om följande sekretessregler inom mitt verksamhetsområde.

Lagrum	Område

Jag är medveten om att jag till någon obehörig inte får föra vidare uppgifter som omfattas av sekretess och att jag kan dömas till ansvar jämlikt 20 kap. 3 § brottsbalken för brott mot tystnadsplikt, om jag röjer eller olovligen utnyttjar en sekretessbelagd uppgift. Jag har också informerats om meddelandefriheten och dess begränsningar i 16 kap. sekretesslagen.

Namnteckning

Sekretessinformationen har meddelats av undertecknad som också bevitnar namnteckningen ovan

Namnteckning 	Namnförtydligande Roger Axelsson	Tjänst Kommissarie
------------------	--	------------------------------

Jag har denna dag fått förnyad upplysning om tystnadsplikten

Ort Göteborg	Datum 2010-01-26	Namnteckning
------------------------	----------------------------	--------------

Från: [Gruppen Skiljande Disciplin Region Väst](#)
Till: [Mats Edsund](#)
Ärende: SV: Ang M ambjörnsson 19830922-6234
Datum: den 8 december 2021 12:16:19
Bilagor: [image001.png](#)
[Scanned from a Xerox Multifunction Printer.pdf](#)
[image002.png](#)
[image003.png](#)

Hej!

Nu har jag varit i kontakt med lite folk.

Beträffande din sista fråga kan du kontakta Sarah Hjortsmarker, chef för mobilitet, så hoppas jag hon kan förklara gällande att få mobiltelefon utan att göra säkerhetsutbildning.

Jag har tidigare begärt ut handlingar gällande Ambjörnsson från personalakten. Det enda de då hade var dokument som rör sekretessinformation, bifogar det här.

Har varit i kontakt med Säkerhetsavdelningen gällande handling "Bekräftelse på genomgången IT-säkerhet". De har inga sådana handlingar kvar hos sig, utan svara att – om vederbörande gått utbildningen – ligger denna i personakten. Denna utbildning har ju tillkommit på senare år, så därför har nog Ambjörnsson inte gått den.

Från Lärplattformen har jag fått skärmdokument på introduktionsutbildning i informationssäkerhet och Mobilitet – grundutbildning – se nedan:

1. Quiz - Riktlinjer	✓ 2021-04-09	Rättat
Godkännande:		
<input checked="" type="checkbox"/> Automatiskt (enligt inställning för delmål)	<input type="button" value="Ångra godkännande"/>	
2. Quiz - Informationssäkerhet	✓ 2021-04-09	Rättat
Godkännande:		
<input checked="" type="checkbox"/> Automatiskt (enligt inställning för delmål)	<input type="button" value="Ångra godkännande"/>	
3. Quiz - Mail och Kalender	✓ 2021-04-09	Rättat
Godkännande:		
<input checked="" type="checkbox"/> Automatiskt (enligt inställning för delmål)	<input type="button" value="Ångra godkännande"/>	
4. Quiz - Kamera	✓ 2021-04-09	Rättat
Godkännande:		
<input checked="" type="checkbox"/> Automatiskt (enligt inställning för delmål)	<input type="button" value="Ångra godkännande"/>	
5. Slutprov	✓ 2021-04-09	Rättat
Godkännande:		

Namn: ☐ [Martin Ambjörnsson](#)

Aktivitet: Introduktionsutbildning i informationssäkerhet

Datum: 2021-12-06

Symboler:

✓ Godkänd

Delmål	Godkänd	Annat
1. Kunskapstest	✓ 2020-01-10	Pågår
Godkännande:		
<input checked="" type="checkbox"/> Automatiskt (enligt inställning för delmål)	(Manuellt godkänt)	<input type="button" value="Ångra godkännande"/>
<input type="button" value="Återställ automatiskt godkännande"/>		
Godkänt av Kristoffer Broberg 2020-01-10		

Hoppas detta var svar på dina frågor.

Med vänlig hälsning

Anita Olsson

Administratör
 GSD Region Väst
 0702-028057

010-56 54063

anita.ohlson@polisen.se**Polisen**

Please think before you print

Från: Mats Edsand**Skickat:** den 1 december 2021 08:21**Till:** Gruppen Skiljande Disciplin Region Bergslagen; Gruppen Skiljande Disciplin Region Väst**Ämne:** Ang M ambjörnsson 19830922-6234

2021-12-06. Förfrågan till Fort-och vidareutbildning

Hejl

Vi behöver hjälp!

Vi måste få in när Martin Ambjörnsson 19830922-6234 genomgick sin sekretessutbildning avseende slagningar i polisen register. När han genomgick Ping-Pong utbildningen?

Vi önskar även de handlingar där Martin Ambjörnsson vid sin anställning skrev under sekretessen. Handlingarna är "Bekräftelse på genomgången IT-säkerhet", "Sekretessinformation" vid anställningen.

Han uppger att efter sin korta tid ifrån Polismyndigheten och när han återanställs så fick han en mobiltelefon utan att göra någon säkerhetsutbildning. Kan detta vara möjligt? Vem kan svara på detta om vi behöver prata med honom/henne?

*Med vänlig hälsning***Mats Edsand**

Kommissarie/ Utredare

Särskilda utredningar Region Väst och Bergslagen

Telefon: 010-56 52818

mats.edsand@polisen.se

Polismyndigheten

Särskilda utredningar, Region Väst/Bergslagen

Telefon till polisen: 114 14

**Polisen**



Polisen

PM 2017:4

Saknr 174

Publicerades den
2017-11-17

Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av it





<i>Avser område/ämne</i> Säkerhet avseende Polismyndighetens informationsbehandling med stöd av it	<i>Gäller för följande organisatoriska enheter (adressater)</i> Polismyndigheten
<i>Beslutad av/titel</i> Dan Eliasson, Rikspolischef	<i>Föredragande/organisatorisk enhet</i> Tomas Landeström, Chef för it-avdelningen
<i>Beslutsdatum</i> 2017-11-17	
<i>Gäller från och med</i> 2017-11-17	<i>Giltighetstid</i>
<i>Ersätter dokument som upphävs</i> Beslut med avseende på bestämmelser för säkerhet vid informationsbehandling med stöd av it, samt användning av it-system inom Polismyndigheten (A098.091/2017).	

INNEHÅLL

1	INLEDNING	5
1.1	Målgrupp och syfte	5
1.2	Omfattning och avgränsning	6
1.3	Läsanvisning	6
1.4	Undantag från riktlinjens krav	6
2	LEDNINGSSYSTEM FÖR IT- OCH INFORMATIONSSÄKERHET	7
3	BEGREPPSSAMLING	8
4	ANSVAR OCH ROLLER.....	10
5	HANTERING OCH SKYDD AV INFORMATION VID INFORMATIONSBEHANDLING MED STÖD AV IT	12
5.1	Informationsskyddsklassning inom Polismyndigheten.....	12
5.2	Behandling av hemliga uppgifter med stöd av it	13
5.3	Informationsutbyte med extern part.....	13
6	RISKANALYS.....	14
6.1	Metod.....	14
7	ANVÄNDNING AV IT-MILJÖN	15
7.1	Generellt om användning av myndighetens it-miljö	15
7.2	Användaridentitet, lösenord och eID-kort.....	15
7.3	Användning av internet.....	16
7.4	Användning av e-post	16
7.5	Användning av sociala medier	16
7.6	Användning av mobil elektronisk utrustning	16
7.7	Distansarbete.....	17
7.8	Hantering av it-utrustning utanför Polismyndighetens lokaler	17
7.9	Användarutbildning	17
8	SÄKER IT – SÄKERHETSASPEKTER FÖR DRIFT OCH INFRASTRUKTUR.....	18
8.1	Driftsäkerhet	18
8.1.1	Generella krav.....	18
8.1.2	Livscykelhantering	18
8.1.3	Systemdokumentation.....	18
8.1.4	Standardkonfiguration och hårdning av systemkomponenter	18
8.1.5	Säkerhetsuppdateringar.....	19
8.1.6	Förändringshantering	19
8.1.7	Felhantering	19
8.1.8	Kapacitetsplanering	19
8.1.9	Säkerhetskopiering	19
8.1.10	Säkerhetsövervakning.....	20
8.1.11	Skydd mot skadlig kod	20
8.1.12	Destruktion av lagringsmedia	20
8.1.13	Avveckling av it-utrustning	20
8.1.14	Klocksynchronisering	21
8.2	Datakommunikation samt nätverk och infrastruktur.....	21
8.2.1	Säkerhetskrav på nätverksmiljön	21
8.2.2	Analys av datakommunikation	21
8.2.3	Trådlösa nätverk	21
8.2.4	Externa nätverk	22
8.2.5	Utrustning och mjukvara	22
8.3	Kryptering och signalskydd	22
8.3.1	Kryptering.....	22
8.3.2	Signalskydd	22

9	ADMINISTRATION OCH STYRNING AV ÅTKOMST	23
9.1	Nationell behörighetsprocess	23
9.2	Generella krav	23
9.3	Tilldelning av behörigheter	23
9.4	Krav på system	24
9.5	Behörighetsrevision	24
9.6	Autentisering av användare	24
9.7	Externa parter behörigheter	25
9.8	Åtkomst utanför skalskyddet	25
10	ANSKAFFNING OCH UTVECKLING	26
10.1	Generella krav	26
10.2	Säkerhetsaktiviteter inför en väsentlig förändring vid utveckling eller anskaffning	26
10.3	Säkerhetsaktiviteter under utveckling eller anskaffning	26
10.4	Säkerhetsaktiviteter vid driftsättning av utvecklad eller anskaffad produkt	27
11	LOGGNING OCH LOGGRANSKNING	28
11.1	Information till användare	28
11.2	Styrning av logghantering	28
11.3	Centralt loggsystem	28
11.4	Övergripande krav på loggning	28
11.5	Lagring och skydd av loggdata	29
11.6	Analys av loggdata	29
11.7	Loggutdrag	29
12	HANTERING AV IT-SÄKERHETSINCIDENTER OCH SÄKERHETSBRISTER	30
12.1	Nationell process för hantering av säkerhetsincidenter	30
12.2	Generella krav	30
12.3	Kommunikation och samverkan	30
13	KONTINUITETSHANTERING	31
13.1	Krav för kontinuitetshantering samt avbrottshantering	31
14	UPPFÖLJNING OCH EFTERLEVNAD	32
14.1	Uppföljning av efterlevnad	32

7 Användning av it-miljön

Hantering i enlighet med detta kapitel ska minimera felaktig användning samt eliminera osäkerhet kring hur myndighetens it-miljö får nyttjas.

7.1 Generellt om användning av myndighetens it-miljö

Dessa generella regler omfattar även användning av mobil elektronisk utrustning.

- 1) It-system² som är tillgängliga inom Polismyndigheten får användas endast när det är nödvändigt för att genomföra en viss arbetsuppgift. Det ska vara sannolikt att användandet i det enskilda fallet är till nytta för arbetets genomförande.
- 2) En medarbetare får inte använda myndighetens it-miljö på ett sådant sätt att it-miljön skadas eller så att andra användares tillgång till it-miljön försvåras.
- 3) En användare som behandlar information på uppdrag av annan användare ska, där så är lämpligt och möjligt, registrera identifieringsuppgifter för den som har beställt uppdraget.
- 4) Endast av it-avdelningen godkänd utrustning får användas för utförandet av tjänsteuppgifter.
- 5) Missbruk av resurser inom myndighetens it-miljö ska anmälas i enlighet med myndighetens rutin för verksamhetsskyddsincidenter.
- 6) Misstankar om brott, eller brottslig verksamhet inom myndigheten ska överlämnas till avdelningen för särskilda utredningar.
- 7) Vid misstanke om brott eller brottslig verksamhet eller missbruk kan användares it-användning granskas eller stängas ner.
- 8) It-system och it-utrustning som Polismyndigheten tillhandahåller är arbetsredskap och myndigheten har, om inte annat i särskilt fall avtalats, rätt att bereda sig tillgång till och förfoga över samtliga i systemen/utrustningen behandlade uppgifter.

7.2 Användaridentitet, lösenord och eID-kort

- 1) Unikt tilldelade användaridentiteter, lösenord och eID-kort är personliga.
- 2) Användare är ansvarig för att inte lämna it-utrustning utan uppsikt på ett sådant sätt att annan kan utnyttja användarens användaridentitet, lösenord eller eID-kort.
- 3) Vid misstanke om att obehörig känner till lösenord ska detta rapporteras enligt it-avdelningens incidenthanteringsprocess, samt lösenordet omedelbart bytas.
- 4) Borttappat eID-kort ska rapporteras till Servicedesk, 020 666 999, för spärning.
- 5) Endast av it-säkerhetsenheten godkända lösenordsdepåer får nyttjas. Med lösenordsdepå avses verktyg för att hantera flertal lösenord.

² För användning av internet och e-post gäller särskilda regler, se avsnitt 7.3 och 7.4

7.3 Användning av internet

- 1) Medarbetarens åtkomst till internet ska användas för arbetsrelaterade arbetsuppgifter. Internetåtkomsten får dock användas även i andra fall under förutsättning att användandet sker i godtagbart syfte och inte stör Polismyndighetens övriga verksamhet.
- 2) Medarbetare som nyttjar åtkomst till internet ska agera säkerhetsmedvetet och inte besöka webbsidor som kan medföra skada för Polismyndighetens anseende eller bedöms innebära säkerhetsrisker för Polismyndighetens it-miljö.
- 3) Det är inte tillåtet att för privat bruk använda av Polismyndigheten tillhandahållen it-utrustning eller internetuppkoppling för att besöka webbplatser som skildrar våld, rasism, pornografi, eller på annat sätt oetiskt eller opassande material.
- 4) Av Polismyndigheten tillhandahållen it-utrustning och internetuppkoppling får ej användas för att sprida politiska, religiösa eller kommersiella budskap.

7.4 Användning av e-post

- 1) Myndighetens e-postsystem ska användas för arbetsrelaterade uppgifter. E-postsystemet får dock användas även i andra fall under förutsättning att användandet sker i godtagbart syfte och inte stör Polismyndighetens övriga verksamhet.
Det är inte tillåtet att använda e-postsystemet på ett sätt som av mottagaren kan uppfattas som någon form av påtryckning eller försök att vinna fördelar. Det innebär att e-postsystemet exempelvis inte får användas vid kontakt med myndigheter eller företag i privata ärenden, om det inte handlar om ärenden av ren administrativ karaktär, exempelvis beställning av varor via en webshop eller motsvarande.
- 2) Det är inte tillåtet att skicka e-postmeddelanden som innehåller våld, pornografi, diskriminerande bilder eller diskriminerande ord, såvida inte arbetsuppgifterna kräver det.
- 3) Myndighetens e-postsystem får inte användas för privata politiska, religiösa eller kommersiella syften.
- 4) Det är inte tillåtet att skicka eller vidarebefordra skräppost eller kedjebrev.
- 5) Det är inte tillåtet att öppna, skicka eller vidarebefordra exekverbara programfiler, såvida det inte krävs för utfarandet av arbetsuppgifter.

7.5 Användning av sociala medier

- 1) Användning av sociala medier (ex. bloggar, Facebook, Twitter, artikelkommentarer m.m.) ska ske i enlighet med Polismyndighetens handledning för polisen i sociala medier.
- 2) Endast information som bedöms vara öppen för allmänheten får offentliggöras via sociala medier.

7.6 Användning av mobil elektronisk utrustning

Med mobil elektronisk utrustning avses bl.a. mobiltelefon, surfplatta eller motsvarande. Bärbar Polar-dator omfattas inte av begreppet.

- 1) Användning av mobil elektronisk utrustning ska ske i enlighet med Polismyndighetens riktlinjer för mobil elektronisk utrustning.

7.7 Distansarbete

- 1) Endast av it-säkerhetsenheten godkända kommunikationslösningar mot myndighetens interna nätverk får användas vid behov av distansåtkomst.
- 2) Informationsägare ansvarar för att godkänna vilka it-system som får användas via distansarbete.

7.8 Hantering av it-utrustning utanför Polismyndighetens lokaler

- 1) It-utrustning som innehåller eller kan ge åtkomst till information med ett högt eller mycket högt skyddsvärde, och som medförs eller används utanför Polisens skalskyddade lokaler ska vara försedd med en av it-säkerhetsenheten godkänd krypteringsfunktion, alternativt vara under ständig uppsikt.
- 2) Personliga Polar-datorer som medförs eller används utanför Polismyndighetens skalskyddade lokaler ska ha så kallad "Pin on boot"³ aktiverat.

7.9 Användarutbildning

- 1) Användarutbildning i it-system som behandlar information med högt eller mycket högt skyddsvärde får endast ske via ett utbildningssystem som behandlar fingerade uppgifter.
- 2) Om det inte är möjligt att utbilda användare med hjälp av fingerade uppgifter i ett utbildningssystem får utbildning endast ske under ledning av godkända handledare.
- 3) Vid utbildning enligt krav 7.9.2 krävs att informationstillgångarnas informationsägare först godkänner utbildningsinsatsen.
- 4) Användarutbildning i it-system som behandlar information med öppet eller ett begränsat skyddsvärde får ske i ett produktionssystem förutsatt att det kan göras utan risk för driftstörningar.
- 5) Samtliga medarbetare ska ta del av myndighetens utbildningspaket avseende it- och informationssäkerhet.

³ Pin on boot innebär att användaren måste ange en pin-kod när datorn startas så att krypteringsnyckeln blir tillgänglig och datorn kan användas.



Bilaga - Skäligen misstänkt

Enhet

Särskilda utredningar, Utredning 1 Göteborg SU

Diariennr

0150-K2050-20

Skäligen misstänkt person		Personnr
Ambjörnsson, Lars Martin		19830922-6234
Identifierad	Kontroll sätt	Kommentar
Ja	Pass (svenskt)	Foto från RES

Misstankeuppgift

Rubricering	Händelse inträffad	Brottskod(Misstanke)
Dataintrång	2019-06-29 14:56 - 2019-06-29 14:57	9466
Brottsplatsadress		Områdeskod
POLISMYNDIGHETEN		9600
Brottsmisstankenr		Diariennr
AM-BM2020-10965-70		0150-K2050-20
Status	Brottskod	Brottsbeskrivning
FU/Utredning pågår	9466	Dataintrång
Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats		
- -		
Underrättelse om misstanke		
2020-11-11		
Lagrum		
4 kap 9 c § 1 st brottsbalken		
Beslutsdatum misstankebeslut	Beslutsfattare misstankebeslut	
2020-10-19	Sundgren, Kajsa	

Misstankeuppgift

Rubricering	Händelse inträffad	Brottskod(Misstanke)
Dataintrång	2019-12-03 13:18 - 2019-12-03 13:19	9466
Brottsplatsadress		Områdeskod
POLISMYNDIGHETEN		9600
Brottsmisstankenr		Diariennr
AM-BM2020-10966-72		0150-K2050-20
Status	Brottskod	Brottsbeskrivning
FU/Utredning pågår	9466	Dataintrång
Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats		
- -		
Underrättelse om misstanke		
2020-11-11		
Lagrum		
4 kap 9 c § 1 st brottsbalken		
Beslutsdatum misstankebeslut	Beslutsfattare misstankebeslut	
2020-10-19	Sundgren, Kajsa	

Misstankeuppgift

Rubricering	Händelse inträffad	Brottskod(Misstanke)
Dataintrång	2019-12-03 14:08 - 2019-12-03 14:09	9466
Brottsplatsadress		Områdeskod
POLISMYNDIGHETEN		9600
Brottsmisstankenr		Diariennr
AM-BM2020-10967-74		0150-K2050-20
Status	Brottskod	Brottsbeskrivning
FU/Utredning pågår	9466	Dataintrång

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

- -

Underrättelse om misstanke

2020-11-11

Lagrum

4 kap 9 c § 1 st brottsbalken

Beslutsdatum misstankebeslut

2020-10-19

Beslutsfattare misstankebeslut

Sundgren, Kajsa

Misstankeuppgift

Rubricering

Dataintrång

Händelse inträffad

2019-12-06 10:03 - 2019-12-06 10:05

Brottskod(Misstanke)

9466

Brottsplatsadress

POLISMYNDIGHETEN

Områdeskod

9600

Brottsmisstankenr

AM-BM2020-10968-76

Diariennr

0150-K2050-20

Status

FU/Utredning pågår

Brottskod

9466

Brottsbeskrivning

Dataintrång

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

- -

Underrättelse om misstanke

2020-11-11

Lagrum

4 kap 9 c § 1 st brottsbalken

Beslutsdatum misstankebeslut

2020-10-19

Beslutsfattare misstankebeslut

Sundgren, Kajsa



Personalia och dagsbotsuppgift

Utskriftsdatum
2022-06-21

Namn Ambjörnsson, Lars Martin		Personnummer 19830922-6234	
Tilltalsnamn Martin	Kallas för	Öknamn	Kön Man
Födelseförsamling Norrstrand	Födelselän Värmlands län	Födelseort utland	
Medborgarskap Sverige	Hemvistland	Telefonnr 0105651105: Arbetstelefon 0722493586: Mobiltelefon	
Adress Jägartorpsvägen 64 A 654 54 Karlstad			
Folkbokföringsort Karlstad		Senast kontrollerad mot folkbokföring 2022-06-17	
Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)			
Utbildning			
Yrke / Titel			
Arbetsgivare		Telefonnr	
Anställning (nuvarande och tidigare)			
Arbetsförhet och hälsotillstånd			
Kompletterande uppgifter			
Uppgiven inkomst 306000	Bidrag	Hemmavarande barn under 18 år 1	
Försörjningsplikt		Skulder 2716000	
Förmögenhet			
Kontroll utförd			
Taxerad inkomst 380000		Taxeringsår 2016	
Taxeringskontroll utförd av		Datum - -	



Underrättelse/Delgivning jml RB 23:18a

Enhet

Särskilda utredningar, Utredning 1 Göteborg SU

Ärende

Diariennr

0150-K2050-20

Handläggare

Edsand, Mats

Gärning

Datainfrång, tilläggsprotokoll

Berörd person

Personnr

19830922-6234

Efternamn

Ambjörnsson

Förnamn

Lars Martin

Underrättelse utsänd

2022-01-27

Yttrande senast

2022-02-11

Underrättelse slutförd

2022-02-11

Delgiven info. om ev. förenklad delgivning

Underrättelsesätt

Per post

Notering

Tilläggsprotokoll

Datum

2022-02-21

Erinran

Se bilaga.

Försvare

Namn

Mats Hellman

Underrättelse utsänd

2022-01-27

Yttrande senast

2022-02-11

Underrättelse slutförd

2022-02-21

Underrättelsesätt

Per post

Notering

Tilläggsprotokoll.

Datum

2022-02-21

Erinran

Se bilaga