Säkerhetsåtgärder vid kameraövervakning

Datainspektionen informerar

Datainspektionen

Säkerhetsåtgärder vid kameraövervakning

Kameraövervakningslagens syfte är att se till så att kameraövervakning kan användas där så behövs samtidigt som enskilda människor skyddas mot otillbörliga intrång i den personliga integriteten. När man använder sig av kameraövervakning, till exempel för att förebygga brott och att förhindra olyckor, är det viktigt att hålla en hög säkerhetsnivå. För att veta vad detta innebär i praktiken har Datainspektionen tagit fram denna checklista över säkerhetsåtgärder och en vägledning för hur säkerhetsarbetet ska bedrivas. Dessutom finns en genomgång av de relevanta bestämmelser som ligger till grund för de bedömningar som måste göras om säkerheten. Informationen vänder sig till alla.

Läs också gärna vår allmänna broschyr Kameraövervakning.

BAKGRUND

Den nya kameraövervakningslagen

Kameraövervakningslagen innehåller en ny samlad reglering av kameraövervakning, oavsett om allmänheten har tillträde till den övervakade platsen eller inte. Det innebär att alla regler om kameraövervakning från och med den 1 juli 2013 finns samlade i en och samma lag. Till den nya kameraövervakningslagen hör en förordning, kameraövervakningsförordningen. Lagen trädde i kraft den 1 juli 2013 och gäller istället för personuppgiftslagen. Lagen ersätter också lagen om allmän kameraövervakning (LAK).

Säkerhetsåtgärder vid kameraövervakning
Maj 2015. Det kan finnas en senare version av den här broschyren i pdf-format på www.datainspektionen.se.
Tryckt hos Ineko, juni 2015 på Arctic Volume White.
Miljömärkt trycksak 341 077. IISSN 1100-3308.

Varför måste man ha en hög nivå på säkerhetsåtgärderna?

Därför att lagen kräver det. Bestämmelser om säkerhetsåtgärder, tystnadsplikt och sekretess i kameraövervakningslagen kräver skyddsåtgärder som ger en hög nivå på skyddet av det inspelade materialet.

Råd för säkerhetsarbetet

Utgångspunkten när det gäller kameraövervakning är att allt bildmaterial som inhämtas genom sådan övervakning anses vara integritetskänsligt till sin natur. Det innebär att kraven på skydds- och säkerhetsåtgärder är höga redan i utgångsläget.

En viktig princip i samband med kameraövervakning är att övervakningen inte får användas för något ändamål som ligger utanför det som man har bestämt från början (finalitetsprincipen). Det innebär till exempel att man inte får använda kameraövervakning som är avsedd för brottsförebyggande ändamål för att även kontrollera de anställdas prestationer eller liknande. Eftersom kameraövervakning i de allra flesta fall sker för att förebygga, avslöja eller utreda brott eller för att förhindra olyckor är det därför endast för dessa ändamål som det är tillåtet att ta del av inspelat bildmaterial från övervakningen.

När ett brott har begåtts behöver man oftast ta fram relevant bildmaterial och överlämna detta till brottsbekämpande myndigheter, till exempel polisen. När en olycka har inträffat handlar det istället om att ta fram bildmaterial för att kunna rekonstruera händelseförloppet så att man kan analysera händelsen och vidta förbättringsåtgärder. I övrigt bör behovet av åtkomst till it-utrustningen endast bestå i att säkerställa att utrustningen fungerar.

Risk- och sårbarhetsanalys

Den som bedriver kameraövervakning bör se över vilka säkerhetsåtgärder som ska vidtas för att upptäcka och skydda bildmaterialet mot obehörig åtkomst eller förlust. För att kunna bedöma vilka säkerhetsåtgärder som är nödvändiga behöver man genomföra en risk- och sårbarhetsanalys. Det finns flera etablerade metoder för det. När man använder dessa metoder, särskilt de som baseras på checklistor, är det viktigt att komma ihåg att det ofta är fråga om generella riktlinjer. Styrkan med metoderna är att någon redan har tänkt igenom olika situationer som kan uppstå. Man får stöd så att inte något viktigt glöms bort. Dessutom går man systematiskt till väga när man arbetar efter en redan fastlagd metod. Det finns leverantörer som erbjuder stöd för att vidta lämpliga åtgärder. Dessa har ofta goda kunskaper på området och är experter på hur man gör för att minska skadan.

Fysisk säkerhet

It-utrustning som används för att behandla och bevara inspelat bildmaterial från kameraövervakning behöver ha ett tillfredsställande skydd mot stöld och andra händelser som kan leda till att det inspelade bildmaterialet från kameraövervakningen sprids till obehöriga eller förstörs.

Den ansvarige behöver därför se över behovet av till exempel:

- låsutrustning till de utrymmen där it-utrustningen förvaras,
- inpasserings- och tillträdeskontroll till de utrymmen där it-utrustningen förvaras,
- galler för fönster till de utrymmen där it-utrustningen förvaras,
- en fungerande larmutrustning som ska skydda mot inbrott.

Det kan ibland uppstå en konflikt mellan olika skyddsåtgärder. Till exempel kan brandskyddskrav på olåsta dörrar komma i konflikt med krav på inpasseringskontroll. Kravet på att begränsa antalet personer som har åtkomst till systemet kan strida mot kravet på personoberoende när

det gäller it-utrustning och system. I sådana situationer måste man vara extra vaksam när man väljer och utformar lämpliga skyddsåtgärder.

Portabel it-utrustning

När man använder portabel it-utrustning, som smartphones, surfplattor och flyttbara lagringsmedia, i samband med kameraövervakning är risken särskilt stor för att utomstående kan komma åt inspelat bildmaterial. Därför ställs det särskilda krav på säkerhet när sådan it-utrustning används. Det ska upprättas rutiner för hur den portabla it-utrustningen och det inspelade bildmaterialet ska förvaras. Inspelat bildmaterial från kameraövervakning som lagras på mobila enheter behöver i normalfallet krypteras.

Tillträdeskontroll

För att säkerställa att endast behörig personal får tillträde till utrymmen där it-utrustning finns behöver rutiner för tillträdeskontroll upprättas. I samband med kameraövervakning gäller att åtkomst till det inspelade bildmaterialet endast ska ges till så många personer som är nödvändigt för att syftet med övervakningen ska kunna nås. I de flesta fall handlar det om ett fåtal personer. Den som bedriver kameraövervakning ska göra en analys av hur många personer som behöver ha åtkomst till bildmaterialet.

I samband med tillståndspliktig kameraövervakning framgår det ofta av villkoren för övervakningen vilken krets av personer som ska ha tillgång till det inspelade bildmaterialet.

Behörighetskontroll

För att förhindra obehörig användning eller åtkomst ska den it-utrustning där inspelat bildmaterial lagras omfattas av ett system för behörighetskontroll när det handlar om större verksamheter. Ett sådant system ska omfatta möjligheter att identifiera användare och bekräfta användarens identitet, exempelvis genom användning av personliga

Den som ansvarar för kameraövervakning behöver se över behovet av till exempel inpasserings- och tillträdeskontroll till de utrymmen där it-utrustningen förvaras.

lösenord. Andra tekniker för identifiering, till exempel engångslösenord, aktiva behörighetskort eller biometriska metoder, till exempel fingeravtryck, kan också användas. Syftet med behörighetskontrollen ska vara att inte fler än vad som är nödvändigt har tillgång till bildmaterialet.

Om bildmaterialet, både inspelat och strömmat, är åtkomligt över ett så kallat öppet nät, till exempel internet, ska identifieringen i första hand ske med hjälp av stark autentisering, till exempel e-legitimation, engångslösenord eller aktiva behörighetskort. Det ska finnas rutiner för tilldelning, ändring, borttagning och kontroll av behörigheter.

Kryptering av till exempel ett lagringsmedium, där krypteringsnycklarna är tillräckligt långa och hanteras på ett säkert sätt, kan användas som skydd även när man vill försäkra sig om att personal som behöver fullständiga rättigheter till systemet inte ska kunna ta del av inspelat bildmaterial från kameraövervakning.

Behandlingshistorik (logg)

För att kunna kontrollera åtkomsten till det inspelade bildmaterialet bör det finnas en behandlingshistorik (logg) som sparas under en viss tid. Några punkter att tänka på är att en behandlingshistorik

- behövs normalt inte om endast en person använder övervakningsutrustningen.
- bör följas upp och skyddas mot otillåtna ändringar.
- bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av inspelat bildmaterial. Behandlingshistoriken bör ange till exempel åtkomst, ändring, utplåning eller kopiering av inspelat bildmaterial.
- bör utformas eller användas så att den inte i sig medför en risk för intrång i användarnas personliga integritet.

En behandlingshistorik har också en förebyggande funktion. Förutsättningen för det är att användarna informeras om att den förs och att den kontrolleras. Det ska finnas en reell upptäcktsrisk för de personer som felaktigt bereder sig åtkomst till det inspelade bildmaterialet.

Inloggning och lösenord

När det gäller inloggning och lösenord behöver man tänka på följande:

- Användaridentitet och lösenord ska inte antecknas där andra kan komma åt uppgifterna.
- Lösenord behöver bytas regelbundet.
- Personlig inloggningsidentitet får aldrig överlåtas till någon annan.
- En skärmsläckare med lösenord behöver användas om inte utloggning alltid sker när en arbetsstation lämnas obemannad, även för en kort tid.
- Lösenord behöver vara långa och det är bra att blanda små och stora bokstäver med siffror.

Kommunikation

För att förhindra att inspelat bildmaterial från kameraövervakning vid överföring förstörs, ändras, kommer i orätta händer eller förvanskas via nät behöver den som bedriver kameraövervakning införa lämpliga åtgärder för att åstadkomma en tillfredsställande säkerhet för överföringen. För att skydda inspelat bildmaterial från kameraövervakning vid lagring mot att förstöras, ändras, förvanskas eller från att komma i orätta händer behöver obehörig åtkomst från internet till it-utrustning eller lokala nät förhindras.

Genom kryptering förhindrar man att uppgifterna kan läsas eller förvanskas i samband med överföringen. För att kryptering ska ge det skydd som krävs ska krypteringen ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt.

Användningen av e-post för att distribuera inspelat bildmaterial innebär stora säkerhetsrisker. Därför bör bildmaterial från kameraövervakning inte skickas okrypterat via e-post. Det kan finnas ytterligare behov av åtgärder och riktlinjer för att minska säkerhetsrisker vid användning av e-post.

Utplåning

När fasta eller löstagbara lagringsmedier som innehåller inspelat bildmaterial från kameraövervakning inte längre behövs för sitt ändamål, alternativt att den längsta bevarandetiden enligt meddelat tillstånd har löpt ut, ska det inspelade bildmaterialet raderas på sådant sätt att uppgifterna inte kan återskapas. Observera att kameraövervakningslagen, till skillnad från äldre bestämmelser, inte tillåter att bevarandetiden förlängs för att bildmaterialet har överlämnats till exempelvis brottsbekämpande myndigheter. Däremot kan det vara tillåtet att vidarebehandla uppgifterna med stöd av andra bestämmelser i annan verksamhet hos den som bedriver kameraövervakning, exempelvis personuppgiftslagen eller den registerförfattning som gäller för den aktuella verksamheten.

Reparation och service

Reparation och service av övervakningsutrustning där material från kameraövervakning hanteras bör ske på ett sådant sätt att bildmaterialet inte blir tillgängligt för obehöriga. När reparation och service av it-utrustning utförs av någon annan än den som bedriver övervakningen bör bildmaterial från kameraövervakning som finns lagrad på it-utrustningen i första hand raderas eller, om det är möjligt, överföras till annat lagringsmedium. Om man inte kan radera materialet, till exempel för att det ska användas senare, bör ett avtal om säkerhet träffas med serviceföretaget. Ett sådant avtal bör till exempel innehålla bestämmelser om vilka säkerhetsrutiner som ska tillämpas. Syftet med avtalet är att det skydd som ska gälla för bildmaterialet kan upprätthållas även om det tillfälligt har överlämnats till någon annan.

Skydd mot skadliga program

Inspelat bildmaterial kan förstöras av skadliga program, så kallad skadlig kod. Användningen av datakommunikation ökar risken för spridning av skadlig kod. Man kan minska risken för att skadlig kod som ofta utnyttjar säkerhetshål i programvaror kan sprida sig i it-utrustningen genom att använda sig av mjukvara från seriösa leverantörer och att ha rutiner för att så snart som möjligt installera programuppdateringar från leverantörerna. Genom att upprätta en särskild policy och rutiner för användande av internet och portabel it-utrustning kan man ytterligare minska risken för att skadliga program kommer in i it-utrustningen.

Verifiering av säkerheten

Regelbundna tester är viktiga om man ska försäkra sig om att säkerhetsorganisationen och it-utrustningen fungerar samt för att hitta eventuella brister i säkerheten. Det finns företag som erbjuder tjänster för detta. Dessa företag har kunskap om var brister kan finnas och de har även den tekniska utrustning som krävs för testerna.

Checklista

Den här checklistan innehåller exempel på lämpliga säkerhetsåtgärder. Den är inte uttömmande och alla punkter behöver inte vara relevanta i alla situationer. Tänk på att det kan finnas behov av ytterligare eller andra åtgärder.

- ☐ Genomför en risk- och sårbarhetsanalys

Skalskydd till de utrymmen där it-utrustningen förvaras

- ☐ Se över låsutrustningen
- ☐ Skaffa inpasserings- och tillträdeskontroll till de utrymmen där it-utrustningen förvaras
- ☐ Säkra alla fönster och dörrar mot intrång
- ☐ Skaffa larm för
  - ☐ Inbrott
  - ☐ Brand
  - ☐ Översvämning
  - ☐ Strömavbrott

Skapa ett behörighetskontrollsystem som

- ☐ begränsar antalet användare
- ☐ identifierar användarna
- ☐ bekräftar användarens identitet

Skydda bildmaterialet mot obehörig åtkomst genom kryptering

- ☐ vid överföring över ett öppet nät
- ☐ vid lagring

Skaffa en behandlingshistorik (loggar) som dokumenterar

- ☐ åtkomst
- ☐ ändring
- ☐ utplåning
- ☐ kopiering

Vid inloggning med lösenord

- ☐ Användaridentitet och lösenord ska inte antecknas där andra kan komma åt uppgifterna.
- ☐ Lösenord behöver bytas regelbundet.
- ☐ Personlig inloggningsidentitet får aldrig överlåtas till någon annan.
- ☐ En skärmsläckare med lösenord behöver användas om inte utloggning alltid sker när en arbetsstation lämnas obemannad, även för en kort tid.
- ☐ Lösenord behöver vara långa och det är bra att blanda små och stora bokstäver med siffror.

Utplåna bildmaterialet

- ☐ senast vid utgången av den tillåtna bevarandetiden
- ☐ vid avveckling av lagringsmedia
- ☐ vid utlämning av lagringsmedia till reparations- och serviceföretag

Om det inte är möjligt att utplåna bildmaterialet

- ☐ Teckna avtal om säkerhetsåtgärder med reparations- och serviceföretaget
- ☐ Skydda it-utrustningen för lagring och inspelning mot skadlig kod med hjälp av antivirusprogram
- ☐ Genomför regelbundna tester av säkerheten

Relevanta bestämmelser i kameraövervakningslagen

Bestämmelser om säkerhetsåtgärder i samband med kameraövervakning finns i kameraövervakningslagen under följande paragrafer.

29 §

Tillgång till ljud- och bildmaterial från kameraövervakning får inte ges till fler personer än vad som behövs för att övervakningen ska kunna bedrivas.

30 §

Den som bedriver kameraövervakning ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda det upptagna bild- och ljudmaterialet. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av
1. de tekniska möjligheter som finns,
2. vad det skulle kosta att genomföra åtgärderna,
3. de särskilda risker som finns med behandlingen av materialet, och
4. hur pass känsligt materialet är.
Om den som bedriver övervakningen anlitar någon annan att ha hand om övervakningen ska han eller hon förvissa sig om att den som anlitas kan genomföra de säkerhetsåtgärder som ska vidtas och se till att åtgärderna verkligen vidtas.

31 §

Den som för någon annans räkning har hand om kameraövervakning får utföra kameraövervakningen bara i enlighet med instruktioner från den som bedriver kameraövervakningen.
Det ska finnas ett skriftligt avtal mellan den som bedriver kameraövervakningen och den som har hand om övervakningen för hans eller hennes räkning. I avtalet ska det särskilt föreskrivas att den som har hand om övervakningen får utföra kameraövervakningen bara i enlighet med instruktioner från den som bedriver kameraövervakningen och att han eller hon är skyldig att vidta de åtgärder som anges i 30 § första stycket.
Om det i lag eller annan författning finns särskilda bestämmelser om behandling av personuppgifter i det allmännas verksamhet i frågor som avses i första stycket, ska i stället de bestämmelserna gälla.

I 37 § kameraövervakningslagen finns dessutom en bestämmelse om tystnadsplikt med följande lydelse.

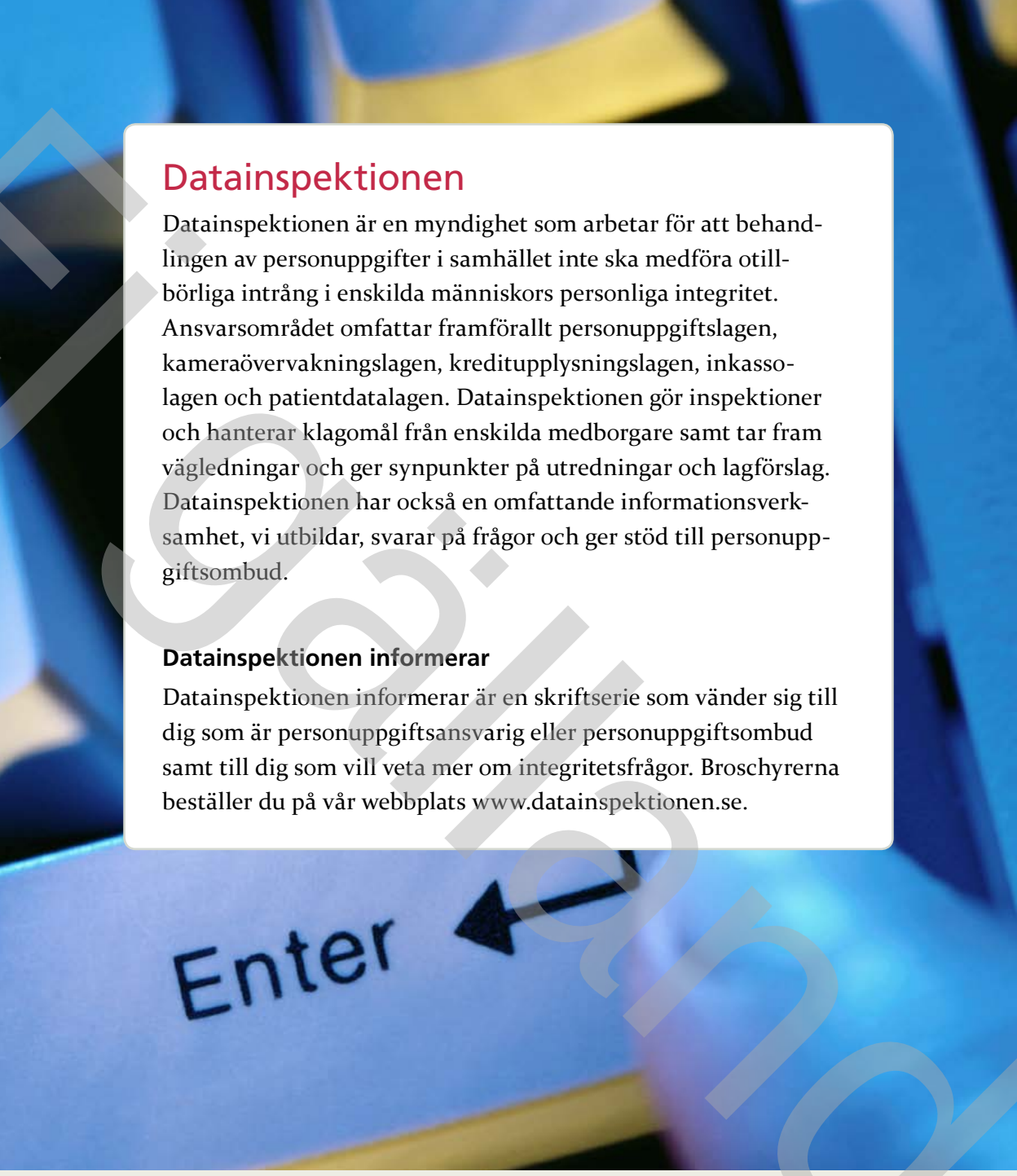
37 §

Den som tar befattning med uppgifter som inhämtats genom kameraövervakning har tystnadsplikt för vad han eller hon genom kameraövervakningen har fått veta om någon enskilds personliga förhållanden. I det allmännas verksamhet ska i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400) tillämpas.

Uppgifter om enskilda som inhämtas genom kameraövervakning har således ett starkt skydd enligt lag. Det innebär att uppgifterna som huvudregel inte får röjas till utomstående annat än i vissa tydligt angivna situationer.

Om du behöver mer information

På Datainspektionens webbplats www.datainspektionen.se kan du läsa mer om kameraövervakning och ladda ner eller beställa informationsmaterial. Där kan du också beställa en prenumeration på Datainspektionens tidning Integritet i fokus och vårt nyhetsbrev.



Datainspektionen

Datainspektionen är en myndighet som arbetar för att behandlingen av personuppgifter i samhället inte ska medföra otillbörliga intrång i enskilda människors personliga integritet. Ansvarsområdet omfattar framförallt personuppgiftslagen, kameraövervakningslagen, kreditupplysningslagen, inkassolagen och patientdatalagen. Datainspektionen gör inspektioner och hanterar klagomål från enskilda medborgare samt tar fram vägledningar och ger synpunkter på utredningar och lagförslag. Datainspektionen har också en omfattande informationsverksamhet, vi utbildar, svarar på frågor och ger stöd till personuppgiftsombud.

Datainspektionen informerar

Datainspektionen informerar är en skriftserie som vänder sig till dig som är personuppgiftsansvarig eller personuppgiftsombud samt till dig som vill veta mer om integritetsfrågor. Broschyrerna beställer du på vår webbplats www.datainspektionen.se.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

Datainspektionen