Konsekvensbedömning/DPIA Kamerabevakning Stadsdelsförvaltningen Hässelby-Vällingbys reception

Steg 1: Identifiera behovet av en konsekvensbedömning:

I dataskyddsförordningen artikel 35.3 anges uttryckligen tre situationer där konsekvensbedömning särskilt ska krävas innan behandlingen påbörjas:

1. En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.
2. Behandling i stor omfattning av särskilda kategorier av uppgifter, eller fällande domar i brottmål och lagöverträdelser som innefattar brott.
3. Systematisk övervakning av en allmän plats i stor omfattning.

Som ett komplement till detta har Integritetsskyddsmyndigheten med stöd av artikel 35.4 publicerat en förteckning över de slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning.[1] I förteckningen anges att nio kriterier ska beaktas för att fastställa om behandlingen är en ”hög risk behandling”. Om två av kriterierna nedan är uppfyllda ska en konsekvensbedömning genomföras:

1. Utvärdering och poängsättning av människor (t.ex. kreditupplysning eller profilering av internetanvändare).
2. Behandling i syfte att fatta automatiserade beslut som har rättsliga eller liknande betydande följder.
3. Systematisk övervakning (t.ex. genom kameraövervakning av allmän plats eller insamling av uppgifter från internetanvändning i offentliga miljöer).
4. Behandlar s.k. särskilda kategorier av uppgifter enligt artikel 9 eller andra uppgifter av mycket personlig

[1] https://www.Integritetsskyddsmyndigheten.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/varfor-konsekvensbedomning/

karaktär (t.ex. patientjournaler, lokaliseringsuppgifter eller bankuppgifter av känslig ekonomisk art).
5. Uppgifter som behandlas i stor omfattning
6. Kombinerande av uppgifter från flera behandlingar på ett sätt som de registrerade inte förväntar sig (t.ex. samkörande av register).
7. Behandling som rör sårbara registrerade (t.ex. barn, asylsökande, anställda, äldre och patienter).
8. Användande av ny teknik eller nya organisatoriska lösningar (t.ex. Internet of Things-applikationer).
9. Behandlingen i syfte att hindra de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal (t.ex. när en bank granskar sina kunder mot en kreditupplysningsdatabas för att besluta om de ska tillåtas att låna).

Beslutet att göra konsekvensbedömning eller inte ska alltid baseras på en helhetsbedömning. Det är med andra ord fullt möjligt att beroende på omständigheterna besluta att *inte* göra konsekvensbedömning trots att två av de nio kriterierna ovan är uppfyllda. Beslutet ska då kunna motiveras och dokumenteras samt dataskyddsombudets råd ska ha inhämtats. Motsatsvis kan det bedömas nödvändigt att göra konsekvensbedömning trots att enbart ett av de nio kriterierna är uppfyllda.

Förklara vad ni syftar till att uppnå med personuppgiftsbehandlingen och vilken typ av behandling det involverar. Sammanfatta varför ni har identifierat ett behov av en konsekvensbedömning.

Det kan vara till hjälp att hänvisa till eller länka till andra dokument, så som projektförslag.

Dokumentera:
Stadsdelsförvaltningen ligger vid Hässelby Torg och är i ett så kallat utsatt område med en problematik kring bland annat narkotikaförsäljning, hot och våld, skadegörelse samt ”häng” i och omkring fastigheten. Kriminella nätverk är starkt förankrade i närområdet. Polisen har kameraövervakning i området pga. upprepad brottslighet.
Receptionen är också välbesökt och det kan vara upp till 600 st. personer som besöker på en dag. Stadsdelsförvaltningen har också flest orosanmälningar, mest behov av hjälp vid psykisk ohälsa och ansökningar om bistånd i hela Stockholm stad. Det gör att flera personer också blir upprörda över beslut, omhändertagna barn osv.

Stadsdelen har under 2019 och 2020 blivit utsatt för ett flertal större incidenter/händelser där personal blivit utsatta för hot och våld samt egendom som blivit föremål för skadegörelse. Exempelvis utsattes lokalen för ett brandattentat, detta med stora kostnader som följd. Förvaltningen utsätts systematiskt för ”attacker” där skadegörelse mot skalskydd, in/ut gångar på fastigheten och tjänstefordon. Personalen hanterar dagligen personer i socialt utsatta situationer där alkohol och narkotika många gånger är inblandade. Personalen möts med hot och våld i deras möten med klienter. Våld och hot mot både vakter och socialsekreterare har ökat och införandet av kamerabevakning blir dels en trygghetsskapande åtgärd i en ibland hård och farlig arbetsmiljö. (Se bilaga 3 händelser.)

Kamerabevakningen syftar till att:

- förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda och lagföra brott på en brottsutsatt plats alternativt på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom.

Enligt Dataskyddsförordningen ska en konsekvensbedömning utföras avseende en kamerabevaknings konsekvenser för skyddet av personuppgifter när typen av kamerabevakning sannolikt leder till en hög risk för de registrerades fri- och rättigheter.
Då kamerabevakning kommer att äga rum på en plats dit allmänheten har tillträde, skulle kamerabevakningen kunna bedömas som särskilt integritetskänslig och kommer även att ske systematiskt. Därför har det beslutats om att en konsekvensbedömning ska göras för att bedöma behovet som finns av kamerabevakning och väga detta mot det motstående integritetsintresset.

Ovan text kan sammanfattas i punkterna 3 och 7:
3. Systematisk övervakning (t.ex. genom kameraövervakning av allmän plats eller insamling av uppgifter från internetanvändning i offentliga miljöer).
7. Behandling som rör sårbara registrerade (t.ex. barn, asylsökande, anställda, äldre och patienter).

Steg 2: Beskriv behandlingen: Tillhandahåll en allmän beskrivning

Beskriv behandlingens karaktär: hur kommer ni att samla in, använda, lagra och radera personuppgifterna? Kommer ni att dela personuppgifterna med någon (vilka är mottagare)? Hänvisa till ett flödesschema eller andra beskrivande dataflöden. Vilka typer av högriskbehandling är inblandade?
Dokumentera: Insamling: Inspelat film-material under kontorstid i reception och i korridor vid besöksrum. Användning: Vid brottsutredning av rättsvårdande myndighet. Lagring: Se bilaga 1 Radering /Gallring: Enligt föreskrift 30 dagar eller enligt gallringsrutin 2016:1. Mottagare: Material kan lämnas ut till polismyndighet vid brottsutredning.
Beskriv behandlingens omfattning: Vilken typ av personuppgifter kommer att behandlas Förekommer s.k. särskilda kategorier av personuppgifter? Förekommer personuppgifter som rör fällande domar i brottmål eller andra känsliga typer av uppgifter? Hur stora volymer av personuppgifter kommer ni att samla in och använda? Hur ofta? Hur länge kommer de att sparas? Hur många enskilda påverkas? Vilket geografiskt område täcker behandlingen?
Dokumentera: Kamerabevakningen kommer att bestå av film. Och kommer spela in mellan vardagar kontorstid mellan 07:00-19:00. Det inspelade materialet kommer endast att användas då ett brott enligt brottsbalken uppdagats, detta innebär att lagringstiden är begränsad. Endast behörig personal får ta del av materialet. Uppgifterna ska spelas över efter 30 dygn men kan sparas längre om det är nödvändigt genom export till lagringsmedium på begäran av rättsvårdande myndighet. Det kan exempelvis röra sig om att filmen behövs för att anmäla ett brott eller för att polisen begär att få ta del av filmen som bevis i en pågående utredning. När filmen inte längre behövs för något av dessa syften ska den raderas alternativt enligt gallringsbeslut SSA 2016:1 senast efter två månader. Motiveringen av tiden 30 dygn är beroende av

tidigare historik då ett möte med tex. ett avslag har triggat och utlöst flera händelser.

Antalet besökare i receptionen varierar per dag mellan 150-600 personer/dag. Antalet som arbetar i stadsdelsförvaltningen och passerar genom receptionen varierar mellan 100-250.

Beskriv behandlingens sammanhang: Vilken typ av relation har ni till de registrerade? Hur stor kontroll kommer de registrerade att ha? Skulle de förvänta sig att ni använder deras personuppgifter på detta sätt? Inkluderar personuppgifterna barn eller andra utsatta grupper? Finns det tidigare bekymmer med denna typ av behandling eller säkerhetsbrister? Är det på något sätt nytt? Hur ser den nuvarande tekniken ut inom det här området? Finns det några aktuella problem av allmänt intresse som bör vägas in? Har ni anslutit er till någon godkänd uppförandekod eller certifieringssystem (när någon sådan har godkänts)?

Dokumentera:
De registrerade som kommer att omfattas av kamerabevakning är anställda vid Stockholms stad samt allmänhet som besöker Stadsdelsförvaltningen.

Insamlingen av personuppgifter kan leda till att barn och personer i särskilt utsatta situationer inhämtas då det är en filmupptagning i ett allmänt utrymme. Dock har avgränsning bestämts att endast vara i korridor och väntrum. Det kommer inte gå att filma inne i besöksrum, toaletter etc. (Se bilaga 2 kamerors placering.) Utanför i trapphus samt i angränsande utrymmen där skalskyddet börjar kommer det inte gå att filma.

Personer som besöker denna typ av anläggning förväntar sig att bli bemötta säkert. Många är där för att få hjälp och ibland också skydd. Man kan därför föreställa sig att det snarare är tvärt om- att området inte är bevakat med kamera som besökaren skulle reagera på. Polisen har också kamerabevakning i anslutning till bygganden där förvaltningen huserar idag.

Tekniken är på intet sätt ny och används i stor utsträckning i samhället. Begränsning kommer att ske i vem som har åtkomst till hårddisk samt behörighet att lämna ut film enligt en skriftlig instruktion.

Beskriv syftet (ändamålet) med behandlingen: vad vill ni uppnå? Vad är den avsedda effekten på enskilda? Vad är

fördelarna med behandlingen – för verksamheten, och i större utsträckning?
Dokumentera: Kamerabevakningen syftar till att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom. Kamerabevakning skulle leda till en ökad trygghet för personal samt besökare till Stadsdelen. Det skulle förebygga skadegörelse vilket i sin tur minskade ekonomiska kostnader samt vid behov även stötta rättsvårdande myndighet i sitt utredningsarbete.
Beskriv de tillgångar som är nödvändiga för behandlingen av personuppgifterna: maskinvara, programvara, nätverk, personer samt handlingar och dess spridningskanaler
Dokumentera: Kamerabevakning för Stadsdelsförvaltningens reception kommer att bestå av 4 st. kameror som är placerade på följande sätt: • En kamera som täcker huvudentré samt samtalsrum med riskpersoner (riskrum) • En kamera *vid* riskrum samt korridor med samtalsrum • En kamera *vid* utgång, kapprum • En kamera *vid* korridor med samtalsrum Upplysning av kamerabevakning kommer att ske genom tydlig skyltning. Se bilaga 1.

Steg 3: Samrådsprocess: Med vilka parter har samråd genomförts?

Överväg med vem samråd bör ske: När det är lämpligt ska synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen inhämtas. – *eller* motivera varför det inte är lämpligt att göra det. Vem i verksamheten organisation bör involveras? Behöver verksamheten be ett personuppgiftsbiträde att assistera? Planerar verksamheten att konsultera informationssäkerhetsexperter eller någon annan expert? Dataskyddsombudet ska alltid rådfrågas
Dokumentera:

Samråd med kommunpolis har ägt rum. Efter händelserna som skett under 2020 riktade mot Stadsdelen Hässelby-Vällingby i form av mordbrand, hot och skadegörelse, anser polismyndigheten att det är befogat med kameror i stadsdelsförvaltningens lokaler.

Dataskyddsombudet har ombetts att granska och delta med sina synpunkter.

MBL genomförs 2021-03-22 och bifogas denna handling i arkivet.

Steg 4: Bedöm nödvändighet och proportionalitet hos behandlingen

Beskriv planerade efterlevnads- och proportionalitetsåtgärder, särskilt:

- *Vad är er lagliga grund för behandling? Uppfyller behandlingen rent faktiskt ert syfte (ändamål och ändamålsbegränsning)?*
- *Finns det något annat sätt att uppnå samma resultat? Hur ska ni förebygga funktionsglidning?*
- *Hur säkerställer ni att personuppgiftskvalitet (riktighet) och minimering av personuppgifter (uppgiftsminimering)?*
- *Lagras uppgifterna under en tidsperiod som är nödvändig och proportionerlig?*
- *Vilken information kommer ni att lämna till enskilda? Hur ska ni hjälpa dem att ta tillvara sina rättigheter (tillgång, rättelse, radering, invändning, begränsning av behandling, dataportabilitet)?*
- *Vilka åtgärder vidtar ni för att säkerställa att personuppgiftsbiträden följer reglerna?*
- *Hur skyddar ni eventuella internationella överföringar?*
- *Förhandssamråd med Integritetsskyddsmyndigheten?*

Dokumentera:

Laglig grund: Kamerabevakningen är nödvändig för att kunna utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Syfte: Ändamålet med kamerabevakning är tydligt definierat som att förebygga, och/eller utreda brott. Då hot och våld mot personal, trots att receptionen är bemannad med ordningsvakter, ökat och otryggheten är hög bland personal så bedöms kamerabevakning vara den åtgärd som är nödvändig för att komma till bukt med problematiken.

Andra sätt: Ökat antal vakter men som kan kännas mer som övervakning och ge ett felaktigt intryck för besökaren.

Riktighet och minimering: Behörighetsbegränsing till utrymme där server står samt skrivna rutiner för service etc.

Proportionalitet och nödvändighet: Uppgifterna kommer att lagras i 30 dagar. Detta för att rättsvårdande myndighet ska hinna agera och skaffa de beslut som krävs för att hämta ut material.

Informationsskyldighet: Den som arbetar eller besöker utrymmet som är aktuellt kommer att upplysas genom uppsatta skyltar. Personalen kommer också att informerad av ledningen.

Personuppgiftsbiträde: N/A

Tredjelandsöverföringar: Det sker inga internationella överföringar.

Förhandssamråd: Förhandssamråd med IMY bedöms inte vara aktuellt då inga kvarstående hög risk för den personliga integriteten kvarstår efter åtgärder införts. Men tillståndsansökan för att kameraövervaka kommer att skickas in till IMY.

Steg 5: Identifiera och bedöm riskerna

	***Beskriv risken och karaktären av potentiell påverkan på enskilda registrerade. Inkludera relevanta verksamhetsrisker vid behov.**	**Sannolik-för skada** Hur stor sannolikhet är att risken fråga realiseras? **Osannolikt, möjligt eller sannolikt**	**Graden av skada** Hur allvarlig skadan för den registrerade personen kan antas bli om risken realiseras? **Minimal, betydande eller allvarlig**	**Övergripande risknivå** Sammanväg-ning av sannolikheten och graden av skada: **Låg, medel eller hög**
1	En utomstående får olovligen åtkomst genom fysiskt intrång i servern där filmen lagras.	Osannolik	Allvarlig	Medel
2	Personuppgifter raderas olovligen	Möjlig	Betydande	Medel
3	Personuppgifter raderas pga. felaktig hantering	Möjlig	Betydande	Medel
4	Servern kan få åtkomst från hackers/ internet	Osannolik	Minimal	Låg
5	Uppdatering/service av systemet görs inte och personuppgifter skadas/ spelas inte in	Möjligt	Betydande	Medel
6	Personuppgifter läcker pga. antagonistiskt angrepp av ”servicepersonal”	Osannolik	Allvarlig	Medel
7	Personalen kan känna sig övervakade i sin tjänsteutövning	Sannolik	Betydande	Medel

8	Personuppgifter sparas längre än 30 dagar	Osannolik	Betydande	Låg
9	Personuppgifter används för annat än syftet beskrivet i konsekvensbedömningen.	Möjlig	Betydande	Medel
10	För många har att hämta ut personuppgifter ur servern.	Möjlig	Betydande	Medel

* *Beskriv och uppskatta riskens ursprung (t.ex.”dataintrång av utomstående”, ”behörig användare sprider uppgifter till utomstående” m.m.), art (t.ex. obehörig åtkomst, oönskad ändring eller att uppgifter försvinner), särdrag och allvar eller mer specifikt, för varje risk (obehörig åtkomst, oönskad ändring och att uppgifter försvinner) ur de registrerades perspektiv:*
Identifiera möjliga konsekvenser och hot för de registrerades rättigheter och friheter vid händelser, såsom obehörig åtkomst, oönskad ändring och förlust av uppgifter, d.v.s. att exempelvis utomstående kan ta del av integritetskänsliga uppgifter i form av patientuppgifter rörande beroendevård.

Steg 6: Identifiera åtgärder för att minska risker

Identifiera och fastställ åtgärder som ni kan vidta för att minska eller eliminera risker som identifierats som medel eller hög risk i steg 5. Målsättningen är att sänka risknivån i fråga om alla identifierade risker så att risknivån kan anses acceptabel utifrån de krav som följer av GDPR (jämför exempelvis artikel 24, 25 och 32 med dess princip om lämpliga tekniska och organisatoriska åtgärder med hänsyn till riskerna).

	Risk/er	**Alternativ för att minska eller eliminera risker**	**Effekt på risk** Eliminerad, reducerad eller accepterad	**Kvarstående risk** Låg, medel eller hög (Acceptabel eller inte, utifrån GDPR:s krav?)	**Åtgärd godkänd** Ja/Nej
1	En utomstående får olovligen åtkomst genom fysiskt intrång i servern där filmen lagras.	• Låst skåp som extra skydd	Reducerad	Låg	JA
2	Personuppgifter raderas olovligen	• Behörighetsbegränsning i själva utförandet	Reducerad	Låg	JA

		• Får endast ske med beslut av direktör.			
3	Personuppgifter raderas pga. felaktig hantering	• Utbildning • Skriftlig rutin • Behörighetshantering	Reducerad	Låg	JA
5	Uppdatering/service av systemet görs inte och personuppgifter skadas/ spelas inte in	• SLA med leverantör av tjänst/ kamera • Skriftliga rutiner	Reducerad	Låg	JA
6	Personuppgifter läcker pga. antagonistiskt angrepp av ”servicepersonal”	• Loggbok (fysisk gästbok) med vem som är inne i systemet. • God kontroll i upphandling av företag.	Reducerad	Låg	JA
7	Personalen kan känna sig övervakade i sin tjänsteutövning	• Skriftlig rutin med vad som får hämtas ut och i vilket syfte. • Tydlig och löpande information till personal. Transparens.	Reducerad	Låg	JA
9	Personuppgifter används för annat än syftet beskrivet i konsekvensbedömningen.	• Skriftlig rutin med vad som får hämtas ut och i vilket syfte.	Reducerad	Låg	JA

10	För många har behörighet att hämta ut personuppgifter ur servern.	• Skriftlig rutin med vad som får hämtas ut och i vilket syfte. • Behörighetsbegränsning	Reducerad	Låg	JA

* Tekniska eller organisatoriska åtgärder för att minska eller eliminera risken ifråga; *exempel på tekniska åtgärder: kryptering (vid överföring och/eller lagring), pseudonymisering, behörighetshantering, loggning och logguppföljning, gallring, förstärkt motståndskraft. Exempel på organisatoriska åtgärder; utbildningsinsatser för att höja medvetenheten, förändrade arbetsrutiner, upprättande av tydliga rutinbeskrivningar, övergång från manuella arbetsrutiner till systembaserade.*

Steg 7: Godkänn och återge resultat

Punkt	Namn/datum	Noteringar
Åtgärder godkända av ansvarig:		Integrera åtgärder i projektplanering och förvaltningsstyrning med datum och ansvar för slutförande.
Kvarvarande risker godkända av:		Vid kvarvarande Hög Risk kontakta Integritetsskyddsmyndigheten för samråd enligt artikel 36 i dataskyddsförordningen.
Dataskyddsombudets råd:	Jessica Hillergård 2021-03-18	Dataskyddsombudet ska ge råd om förenlighet och se över informationen i de 6 stegen ovan (övervaka) samt därefter ge besked om behandlingen kan påbörjas eller fortsätta.
Sammanfattning av dataskyddsombudets råd: Dataskyddsombudet ger råd att följa de åtgärder som tagits fram i steg 6 för att minska de risker som tagits fram i steg 5. Konsekvensbedömningen ska ses över årligen av säkerhetssamordnare och Dataskyddsombud och vid behov uppdateras och föredras för personuppgiftsansvarig.		
Dataskyddsombudets råd accepterat eller avvisat av:		Om Dataskyddsombudets förslag avslås måste motivering ges.
Motivering:		
Samrådssvar bedömda av:		Om beslut utgår från enskilda samrådssvar t.ex. registrerade, arkivarie, IT-säkerhetsansvarig m.fl. måste motivering/summering lämnas.
Summering av samrådssvar:		
Konsekvensdömning genomförd av:	• Amir Farihadi Säkerhetssamordnare	Ansvarig för genomförd konsekvensbedömning. Bedömningar ska periodiskt

	• Ann Ulin Verksamhets controller avdelningen Vuxna • Ann Stolpe Informationssäkerhets-samordnare • Per Onning Trygghetssamordnare • Tommy Ordningsvakt	följas upp och eventuellt revideras. Dataskyddsombudet bör även granska att den ansvarige agerar i enlighet med konsekvensbedömningen

Konsekvensbedömningen ska sparas och diarieföras samt vid behov uppdateras enligt dataskyddsförordningen.

Western Digital

WD Purple™

DATA SHEET — SURVEILLANCE HARD DRIVES

WD Purple™ drives are built for 24/7, always-on, high-definition security systems. WD Purple™ surveillance storage feature Western Digital's exclusive AllFrame™ technology, so you can confidently create a security system tailored to the needs of your business. Using AllFrame™ technology, WD Purple™ drives improve video capturing and helps to reduce errors, pixelation, and video interruptions that could happen in a video recorder system. WD Purple drives have an enhanced workload rating that supports systems designed for 24×7 video recording with up to 64 cameras.

Highlights

- Capacity up to 12TB
- Support for up to 64 cameras per drive
- AllFrame™ technology
- Up to 16 AI channels for Deep Learning analytics on AI-enabled NVRs (10TB & 12TB capacities)
- MTBF of up to 1.5 million hours
- 3-year limited warranty

INTERFACE
SATA 6 Gb/s

PERFORMANCE CLASS
5400 / 7200 RPM Class

FORM FACTOR
3.5-inch

CAPACITIES
1TB to 12TB

MODEL NUMBERS

WD10PURZ	WD40PURZ	WD81PURZ
WD121PURZ	WD20PURZ	WD60PURZ
WD100PURZ	WD30PURZ	WD80PURZ
WD101PURZ		

THE WESTERN DIGITAL ADVANTAGE

Western Digital puts our products through extensive Functional Integrity Testing (F.I.T.) prior to any product launch. This testing ensures our products consistently meet the highest quality and reliability standards of the Western Digital brand.

Western Digital also has a detailed Knowledge Base with more than 1,000 helpful articles as well as software and utilities. Our customer support lines have long operational hours to ensure you get the help you need when you need it. Our toll-free customer support lines are here to help, or you can access our Western Digital Support site for additional details.

Industry-leading storage. Surveillance you can trust.

Western Digital is a worldwide leader in the hard drive industry. With WD Purple surveillance storage, you have a drive engineered for high temperature, always-on surveillance systems so you can rely on quality video playback when you need it most. Whether you're protecting loved ones or monitoring your business, WD Purple offers performance you can trust.

Western Digital's Exclusive AllFrame Technology

All WD Purple drives are equipped with AllFrame technology, which improves ATA streaming to help reduce frame loss, improve overall video playback, and increase the number of hard drive bays supported within a NVR. Help make your surveillance solution future-ready knowing that WD Purple drives are ready for ultra high definition cameras. WD Purple capacities up to 8TB feature AllFrame 4K technology enabling high quality recording for up to 64 cameras. WD Purple 10TB and 12TB capacities feature AllFrame AI technology that enables not only recording up to 64 cameras, but also an additional 32 streams for Deep Learning analytics within the system.

Enhanced Workload Ratings

WD Purple drives with AllFrame 4K technology feature a workload rating of up to 180TB/year - up to three times that of desktop drives – to handle the unique demands of modern video surveillance DVR and NVR systems. WD Purple 10TB and 12TB drives with AllFrame AI feature a workload rating up to 360TB/year to support the Deep Learning analytics that are features in AI capable NVRs.

Expand your view to 64

Each WD Purple drive is optimized to support up to 64 cameras. With so many options, you have the flexibility to upgrade or expand your security system in the future.

Designed for Today's and Tomorrow's Surveillance Solutions

With an MTBF of up to 1.5 million hours[1], WD Purple drives are engineered for mainstream surveillance DVRs and NVRs that operate 24/7. With support for more than eight bays[2] and tarnish resistant components[3], WD Purple drives deliver reliable operation in large scale surveillance systems in harsh environments.

Field-proven High Capacity

Now on its 4th generation and with more than 27 million drives shipped[4], field-proven HelioSeal™ technology delivers trusted high-capacity WD Purple storage (8TB, 10TB, and 12TB) for the massive storage needs of 4K surveillance video.

Wide Compatibility. Seamless Integration.

WD Purple hard drives are built with compatibility in mind, so you can quickly and seamlessly add capacity to your surveillance system. With a wide range of industry-leading enclosures and chipsets supported, you're sure to find the DVR or NVR configuration that's right for you.

Low Power. High efficiency.

With our exclusive IntelliSeek™ technology, WD Purple drives are able to calculate optimum seek speeds. This keeps power consumption low so ambient noise and vibrations are at a minimum.

Three Year Limited Warranty

As an industry-leading hard drive manufacturer, WD stands behind their surveillance storage solutions with a 3-year limited warranty included with every WD Purple drive.

Bilaga 1.

HIKVISION

DS-7600NI-K2/P Series NVR

Features and Functions

Professional and Reliable

- Dual-OS design to ensure high reliability of system running
- ANR technology to enhance the storage reliability when the network is disconnected

HD Input

- H.265/H.264/H.264+/MPEG4 video formats
- Connectable to the third-party network cameras
- Up to 16 IP cameras can be connected
- Recording at up to 8 MP resolution
- Supports live view, storage, and playback of the connected camera at up to 8 MP resolution

HD Output

- HDMI and VGA independent outputs provided
- HDMI Video output at up to 4K (3840 × 2160) resolution

HD Storage

- Up to 2 SATA interfaces connectable for recording and backup
- Storage space effectively saved by 50% to 70% with the use of H.264+ decoding format

HD Transmission

- 1 self-adaptive 10M/100M/1000 Mbps network interface
- 8/16 independent PoE network interfaces are provided

Various Applications

- Centralized management of IP cameras, including configuration, information import/export, real-time information display, two-way audio, upgrade, etc.
- Connectable to smart IP cameras from Hikvision and the recording, playing back, and backing up of VCA alarms can be realized
- VCA detection alarm is supported
- Instant playback for assigned channel during multi-channel display mode
- Smart search for the selected area in the video; and smart playback to improve the playback efficiency
- Supports HDD quota and group modes; different capacity can be assigned to different channels.

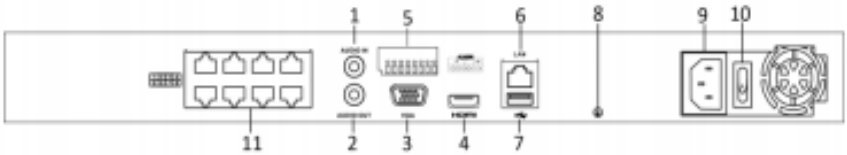
www.hikvision.com

Specifications

Model		DS-7608NI-K2/8P	DS-7616NI-K2/16P
Video/ Audio input	IP video input	8-ch	16-ch
	Incoming bandwidth	80 Mbps	160 Mbps
	Outgoing bandwidth	160 Mbps	
Video/ Audio output	HDMI output resolution	4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
	VGA output resolution	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
	Audio output	1-ch, RCA (Linear, 1 KΩ)	
Decoding	Decoding format	H.265/H.264/H.264+/MPEG4	
	Recording resolution	8MP/6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF	
	Synchronous playback	8-ch	16-ch
	Capability	2-ch @ 4K, or 8-ch @ 1080p	
Network management	Network protocols	TCP/IP, DHCP, HIK Cloud P2P, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS	
Hard disk	SATA	2 SATA interfaces for 2HDDs	
	Capacity	Up to 6TB capacity for each disk	
External interface	Two-way audio	1-ch, RCA (2.0 Vp-p, 1kΩ)	
	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface	
	USB interface	Front panel: 1 × USB 2.0; Rear panel: 1 × USB 3.0	
	Alarm in/out	4/1	
POE Interface	Interface	8 RJ-45 10/100 Mbps self-adaptive Ethernet interfaces	16 RJ-45 10/100 Mbps self-adaptive Ethernet interfaces
	Power	≤ 120 W	≤ 200 W
	Supported standard	IEEE 802.3 af/at	
General	Power supply	100 to 240 VAC	
	Power	≤ 180 W	≤ 280 W
	Consumption (without hard disk)	≤ 15 W	
	Working temperature	-10 to +55° C (14 to 131° F)	
	Working humidity	10 to 90 %	
	Chassis	385 mm chassis	
	Dimensions (W × D × H)	385 × 315× 52 mm (15.2" × 12.4" × 2.0")	
	Weight (without hard disk)	≤ 3 kg (6.6 lb)	

HIKVISION

Physical Interfaces



NOTE

The DS-7616NI-K2/16P and DS-7632NI-K2/16P provide 16 network interfaces with PoE function.

Index	Description	Index	Description
1	AUDIO IN	7	USB 3.0 Interface.
2	AUDIO OUT	8	GND
3	VGA Interface	9	100 to 240 VAC power supply
4	HDMI Interface	10	Power Switch
5	Controller Port, Alarm In/Alarm Out	11	Network Interfaces with PoE function
6	LAN Network Interface		

Available Models

DS-7608NI-K2/8P, DS-7616NI-K2/16P.

Distributed by

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
overseasbusiness@hikvision.com

Hikvision USA
T +1-909-895-0400
sales.usa@hikvision.com

Hikvision Europe
T +31-23-5542770
saleseuro@hikvision.com

Hikvision Middle East
T +971-4-8816086
salesme@hikvision.com

Hikvision Russia
T +7-495-669-67-99
saleru@hikvision.com

Hikvision India
T +91-22-28469900
sales@pramahikvision.com

Hikvision Italy
T +39-0438-6902
info.it@hikvision.com

Hikvision France
T +33(0)1-85-330-444
info.fr@hikvision.com

Hikvision Spain
T +34-91-737-16-55
info.es@hikvision.com

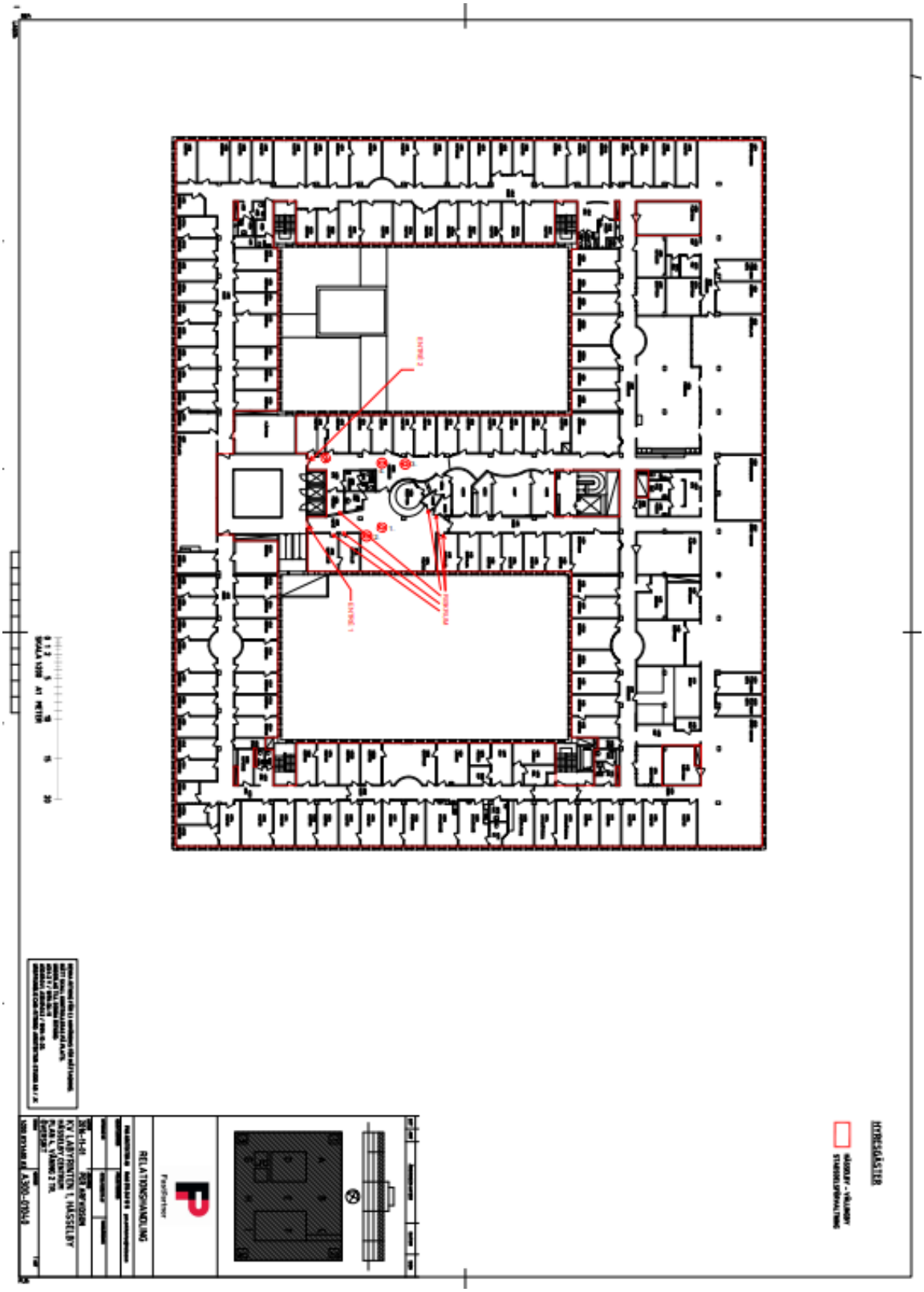
Hikvision Poland
T +48-22-460-01-50
poland@hikvision.com

Hikvision UK
T +44-1628-9021-4
support.uk@hikvision.com

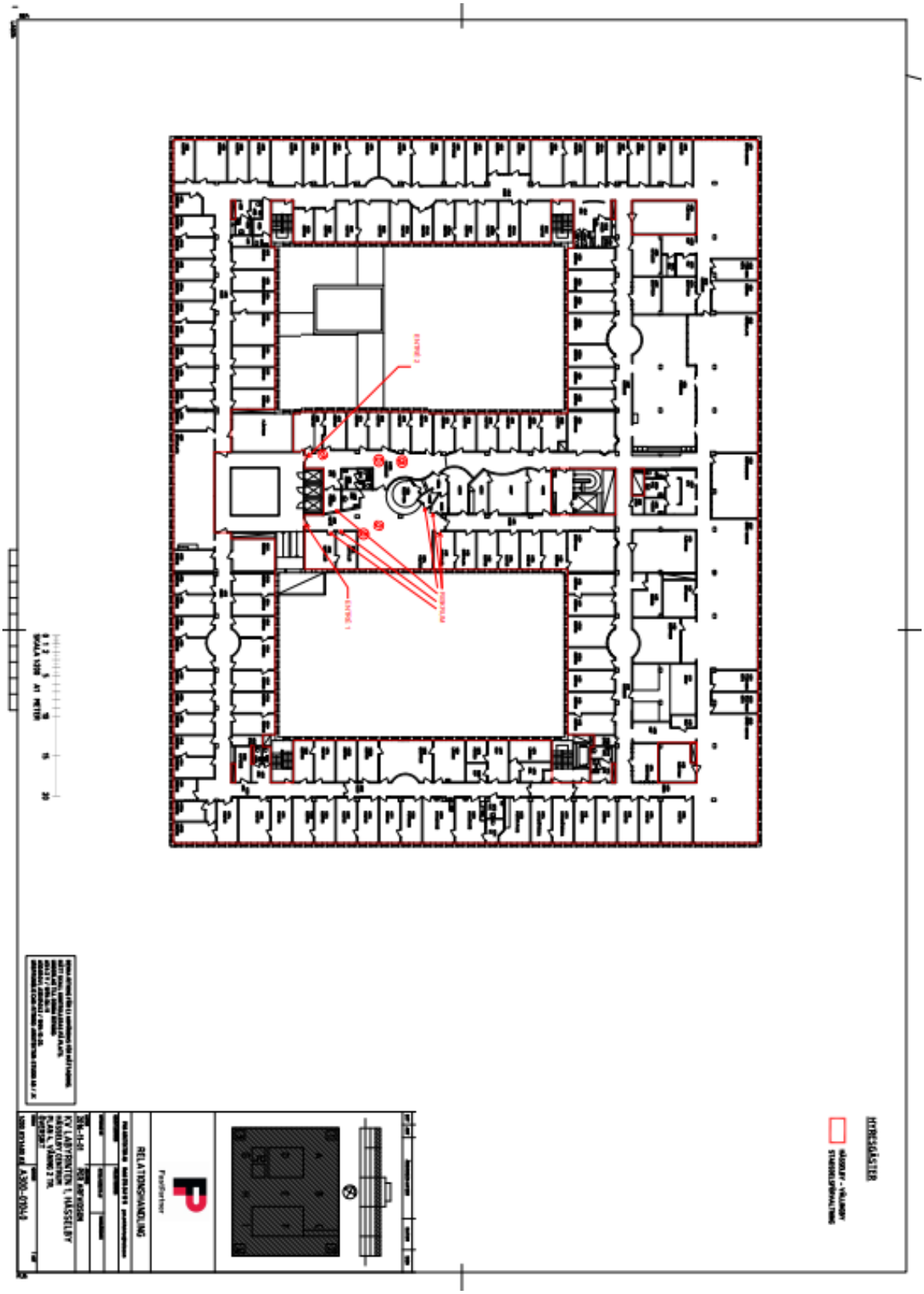
Hikvision Singapore
T +65-6684-4718
sg@hikvision.com

Hikvision Oceania
T +61-2-8599-4233
salesau@hikvision.com

Hikvision Hong Kong
T +852-2151-1761



Bilaga 3.



Konsekvensbedömning/DPIA
Kamerabevakning Stadsdelsförvaltningen
Hässelby-Vällingbys recepl

Grön yta representerar den area allmänheten har obegränsad åtkomst till under kontorstid. Röd yta är de utrymmen som man endast kommer till med följeslagare från stadsdelsförvaltningen.

Allmänt

Hässelby-Vällingby Stadsdelsförvaltning är en mångfacetterad stadsdel med en lika mångfacetterad del av invånare som besöker stadsdelsförvaltningen. Detta ger vid handen en rad utmaningar i de problem som invånarna besöker stadsdelsförvaltning för och ordningsvakterna på plats står inför att hantera. Många händelser de-eskaleras av genom ingripanden av ordningsvakter på plats och många händelser därutav skulle kunna vara föremål för anmälan om hot gentemot uniformerad personal eller stadsdelsförvaltningens anställda eller skadegörelse men där ord står mot ord och sådan anmälan uteblir.
En kameraövervakning av de delar dit allmänheten har tillträde skulle ha en förebyggande effekt på de invånare som besöker stadsdelsförvaltningen men även utgöra en avgörande del i de fall man gör en anmälan av något slag.

Sammanställning större incidenter/händelser 2019/2020

2020

Oktober
- Handläggare ofredas i fastighetens trapphus i anslutning till entrén till stadsdelsförvaltningen av klient (ej dennes klient) genom att denne får någon form av vätska kastad över sig.

Juli
- Man påträffas med spritflaska innan möte med handläggare, avkrävs denna för att möte skall komma tillstånd med handläggare.
- Sjukdomsfall där litet spädbarn avlider.

Juni
- Anlagd brand i trapphus riktat mot stadsdelsförvaltningen.
- Man avvisad efter att ha blivit verbalt och fysiskt utåtagerande i receptionen.
- Kortläsare till stadsdelsförvaltningen vandaliserade.

Maj
- Stadsdelsförvaltningens bilar får däcken sönderskurna.
- Man som varit verbalt och fysiskt utåtagerande mot handläggare avvisas från receptionen.

Februari
- Verbalt utåtagerande och hotfull man talas till rätta i väntdelen – receptionen.

Barn befinner sig i samma del och tar väldigt illa vid sig av mannens hotfullhet och dennes utåtagerande verbalt.

2019

December

- Man som blir verbalt och fysiskt utåtagerande efter mottaget besked vid stängning, avvisas i samarbete med Sthlm Stad mobila ordningsvakter
- Skadegörelse av vattenautomat efter negativt besked om hjälp.
- Man avvisad efter uppträtt hotfullt i receptionen.
- Man avvisad efter uppträtt hotfullt i receptionen.

November

- Man som blir verbalt och fysiskt utåtagerande vid stängning avlägsnas.
- Kvinna som sökt hjälp av RVT (Relationsvåldsteamet) blir attackerad av sin fd man i receptionen.
- Klient som blir fysiskt utåtagerande i besöksrummet och verbalt utåtagerande mot handläggarna. Rusar skrikande ut i korridoren.
- Klient som blir verbalt och fysiskt utåtagerande i receptionen efter mottaget besked. Blir avlägsnad.

Oktober

- Hissdörr i fastighet vandaliserad
- Verbalt utåtagerande och hotfull klient mot handläggare under möte.

Juli

- Bråk mellan klienter under möte med handläggare
- Hot mot tjänsteman. Man som är utåtagerande och hotfull. Skadegörelse av utrustning i receptionen.