Personuppgiftspolicy för TiksPac

För alla anställda och kunder – rörande behandling av personuppgifter

Version	Datum	Ändrad av	Fastställd av
1.1	2018-06-25	Johan Nilsson	VD, Stefan Arvidsson

Innehållsförteckning

Personuppgiftspolicy for TiksPac

Detta dokument har två syften: För det första som ett praktiskt instrument i företagets arbete med att skydda personuppgifter, för det andra som en skriftlig dokumentation av våra ansträngningar att efterleva lagkraven enligt dataskyddsförordningen (GDPR). Genom detta dokument försäkrar vi våra kunder, leverantörer, anställda, partners och andra intressenter att vi gör allt vi kan för att skydda och behandla deras data i enlighet med gällande lagstiftning och sed.

TiksPac's personuppgiftspolicy är utvecklad tillsammans med företagets övergripande strategi, värderingar och visioner och är därmed en integrerad del av hur företaget arbetar. Policyn är fastställd av ledningen och alla medarbetare är medvetna om den och deras ansvar i samband med behandlingen av personuppgifter. Vid misstanke om att personuppgifter inte hanteras korrekt, kontakta snarast till din närmaste chef och informera honom/henne om vad som skett.

Denna personuppgiftspolicy revideras och uppdateras minst en gång per år av ledningsgruppen. Vid nyanställning görs samtliga nyanställda medvetna om denna policy och de måste bekräfta att de tagit del av den genom att signera anställningsavtalet. Det undertecknade anställningsavtalet förvaras hos personalavdelningen i den anställdes personalakt.

Tillsammans med denna personuppgiftspolicy, har en IT-policy utvecklats, som hanterar de mer tekniska aspekterna kring behandling av personuppgifter, inklusive förberedelser för eventuella säkerhetsincidenter. Utöver detta har en registerförteckning upprättats. Denna förvaras hos och hålls uppdaterad av Personuppgiftsansvarig på TiksPac.

1. Definitioner

TiksPac behandlar personuppgifter i samband med inköp, försäljning, marknadsföring, samarbeten och HR frågor. Nedan definieras några av de huvudbegrepp som förekommer i samband med personuppgiftsförordningen för att underlätta förståelsen för personuppgiftspolicyn.

GDPR	The General Data Protection Regulation, Dataskyddsförordningen på svenska är den lag som efter den 25 maj 2018 kommer att reglera behandlingen av personuppgifter.
Personuppgifter	All information om en identifierad eller identifierbar fysisk person såsom t. ex namn, adress, telefonnummer, personnummer, foton mm. Information om enskilda firmor är också personuppgifter.
Känsliga personuppgifter	Som känsliga personuppgifter räknas enligt förordningen bland annat, hälsouppgifter, fackföreningsmedlemskap, ras/etnicitet, politisk åskådning, filosofisk övertygelse, religion, genetiska eller biometriska data.
De registrerade	Alla personer vars information behandlas hos TiksPac, t. ex kunder, anställda och leverantörer.
Behandling (av personuppgifter)	Allt som företaget gör med personuppgifterna, inkluderat lagring och radering.
Personuppgiftsansvarig (Data Controller)	Den som beslutar om syfte, omfattning och metoder för behandling av personuppgifter, i detta fall TiksPac AB, 556856-0063
Personuppgiftsbiträde (Data Processor)	Den som hanterar personuppgifter på uppdrag av den personuppgiftsansvarige, t. ex löneadministration, molntjänster, och transportörer.

2. Organisation och ansvar

TiksPac är indelat i olika enheter. Denna personuppgiftspolicy gäller för samtliga delar av organisationen men det kan i vissa fall vara nödvändigt att ha specifika regler i specifika delar. I de fall specifika regler

krävs måste dessa regler stämma överens med denna policy, ha en tydlig uppdelning av roller och ansvar och en fastställd plan för revidering.

Ansvaret för att de anställda följer denna personuppgiftspolicy ligger främst hos de anställda själva, därefter hos deras närmaste chefer. Kontroller av efterlevnaden av denna policy ska genomföras och resultatet av dessa revisioner ska dokumenteras och förvaras hos personuppgiftsansvarig. Om det vid kontroller visar att det förekommit incidenter där denna personuppgiftpolicy inte följts, är det i första hand den närmaste chefens uppgift att åtgärda dessa incidenter. Avdelnings/bolagschefer måste också genomföra regelbundna uppföljningar och rapportera till personuppgiftsansvarig vid företaget som har det övergripande ansvaret för personuppgiftspolicyn.

3. Instruktioner till anställda

Nedan följer specifika regler och riktlinjer som alla anställda vid TiksPac måste följa i samband med behandling av personuppgifter. Dessa instruktioner och riktlinjer är baserade på de legala krav som finns i dataskyddsförordningen (GDPR) och utgör tillsammans med IT-Policy och övriga dokument rörande personuppgiftsbehandling grunden till företagets strävan att efterleva förordningen. Varje del av instruktionen är uppdelad i **syfte** (varför gör vi det), **riktlinjer** (hur gör vi det) och **kontroll** (hur har vi faktiskt gjort det).

3.1 Laglig Grund

Syfte:

- Det finns laglig grund för all personuppgiftsbehandling

Riktlinjer:

Innan en behandling av personuppgifter påbörjas måste den lagliga grunden för behandlingen fastställas. Detta genomförs av processägaren i samråd med avdelningschefen. Dataskyddsförordningen specificerar sex olika fall av laglig grund;

- Samtycke
- Fullgöra avtal
- Rättslig förpliktelse
- Vitala intressen
- Allmänt intresse och myndighetsutövning
- Berättigat intresse.

Som regel använder företaget *berättigat intresse* rörande kunder och presumtiva kunder samt samtycke och fullgörande av avtal för anställda, leverantörer och etablerade kunder. Skulle det uppstå frågetecken eller osäkerheter kring den lagliga grunden, kontakta din närmaste chef eller den personuppgiftsansvarige vid företaget. Om laglig grund inte kan identifieras skall inte behandling av personuppgifterna påbörjas.

I de fall känsliga personuppgifter behandlas utöver kraven för anställningen, måste den lagliga grunden alltid vara samtycke.

I de fall personuppgifter om barn under 13 år behandlas, skall samtycket ges av barnets föräldrar.

Den lagliga grunden för behandlingen av personuppgifterna ska dokumenteras tillsammans med de relevanta processerna i registerförteckningen.

Signerade /accepterade samtyckeshandlingar ska förvaras hos personuppgiftsansvarig.

Kontroll:

Exempel på kontroller:

Samtliga behandlingar revideras årligen, inkluderat den lagliga grunden.

3.2 Uppgiftsminimering och ändamålsbegränsning

Syfte:

- Informationen som samlas in baseras på ett tydligt syfte och vi samlar inte in mer information än vad som verkligen krävs.

Riktlinjer:

För varje behandling ska det finnas klart definierade riktlinjer kring vilka personuppgifter som är relevanta i förhållande till syftet vilket också säkerställer att inte mer uppgifter än vad som verkligen är nödvändigt samlas in. Syftet med behandlingen och vilka typer av personuppgifter som behandlas ska vara definierat i registerförteckningen.

I de fall då det kan ligga i företagets intresse att samla in mer uppgifter än vad som nödvändigtvis behövs, måste det finnas ett dokumenterat samtycke.

Kontroll:

Exempel på kontroller:

Alla behandlingar revideras årligen, de insamlade kategorierna av personuppgifter jämförs med syftet för att säkerställa att uppgifterna fortfarande behövs för att uppnå syftet.

Ansvariga chefer måste genomföra slumpvisa kontroller i CRM systemet en gång i månaden för att kontrollera om behandlingen innehåller mer uppgifter än vad som är relevant för syftet. Om systemet innehåller mer uppgifter måste ett samtycke inhämtas från den registrerade.

3.3 Korrekthet och Öppenhet

Syfte:

- Att säkerställa transparens kring företagets behandling av personuppgifter samt att säkerställa att de registrerade är medvetna om sina rättigheter.

Riktlinjer:

Vid tidpunkten för anställning ska de anställda på ett lättförståeligt sätt genom deras anställningskontrakt informeras om:

- Vem som är personuppgiftsansvarig och dennes kontaktuppgifter
- Syftet med personuppgiftsbehandlingar
- Laglig grund för behandling samt berättigade intressen som används av företaget
- Vilka andra mottagare som finns av företagets personuppgifter samt eventuella överföringar till tredje land
- Gallringstiden för personuppgifter
- Den registrerades rättigheter i förhållande till personuppgifter (rätt till tillgång, rättelse av uppgifter, radering av uppgifter, begränsning av behandling och dataportabilitet)
- Rätten att ta tillbaka ev. samtycke
- Rätten att klaga hos tillsynsmyndigheten
- Om att de är skyldiga att informera och vilka konsekvenserna kan bli om man inte informerar
- Hur informationen samlas in om den inte kommer direkt från den registrerade
- Eventuell omfattning av automatiserat beslutsfattande och logiken bakom denna

Om företaget senare vill behandla personuppgifter i ett annat syfte än vad som tidigare uppgetts till den registrerade, måste den registrerade informeras om detta innan behandlingen påbörjas.

För att informera kunder och berörda läggs en sammanfattning av företagets hantering av personuppgifter samt denna personuppgiftspolicy ut på företagets hemsida. En länk till denna policy skickas elektroniskt till den registrerade vid första kontakten.

Kontroll:

Exempel på kontroll:

Det är avdelningschefernas ansvar att verifiera att man följer kraven på vilken information som ska delges. Det mesta av informationen säkerställs att den delges genom att den finns på hemsidan, men vid direktkontakt via mail skall en länk till informationen bifogas. Detta email är kvittot på att vi följer kraven på att informera och måste arkiveras tillsammans med övrig kundinformation. Regelbundet granskas öppna kundcase för att säkerställa att kravet på information efterlevs.

3.4 Rätten till tillgång

Syfte:

- Att säkerställa att den registrerade kan få tillgång till den information som behandlas om honom/henne

Riktlinjer:

Vid förfrågan, skall den registrerade utan onödigt dröjsmål få tillgång till, på ett lätt läsbart sätt, den information som finns sparad om personen, omfattande:

- Syftet med behandlingen
- Vilka kategorier av uppgifter som behandlas
- Ev. andra mottagare av informationen, inklusive överföringar till tredje land
- Lagringstiden för uppgifterna
- Den registrerades rättigheter i förhållande till sina personuppgifter (tillgång, rättning, radering, begränsad behandling och dataportabilitet)
- Rätten att lämna in ett klagomål till tillsynsmyndigheten
- Hur företaget fått uppgifterna om de inte tillhandahållits direkt av den registrerade
- Omfattningen av ev. automatiserat beslutsfattande och logiken bakom detta

En anställd som mottar en sådan begäran ska kontakta den personuppgiftsansvarige vid företaget så snart som möjligt. Informationen ska tillhandahållas i pappersformat eller i lättanvänt elektroniskt format baserat på det format den registrerade vill ha.

Det måste säkerställas att personen som mottar uppgifterna verkligen är rätt person. Informationen får bara delges när personen har identifierat sig själv eller har på annat sätt säkerställt att personen som begär tillgång faktiskt är den person som informationen berör eller att hen har fullmakt från den personen.

Telefonförfrågningar

Vid telefonförfrågningar, måste det säkerställas att information delges rätt person. Till exempel kan det vara nödvändigt att ställa kontrollfrågor, t. ex fråga om adress eller personnummer, eller motringa personen. Om den anställde inte kan garantera identiteten, måste informationen skickas via brev till den registrerades folkbokföringsadress för att minska risken för bedrägerier.

Förfrågningar via brev och e-mail

Om namnet och adressen på brevet/e-mailet är identiskt med den tidigare registrerade informationen i systemet, kan informationen vanligtvis skickas till den registrerade adressen. Om detta inte är fallet måste ärendet undersökas vidare innan informationen delges.

Tillgång till information på uppdrag av annan (Fullmakt)

Den registrerade kan ge någon annan fullmakt att få tillgång till hans/hennes information. Fullmakten kan vara specifik eller generell.

Vid osäkerhet om fullmakten är tillräcklig måste företagsledningen/jurist tillfrågas.

Kontroll:

Exempel på kontroll:

Förfrågningar om tillgång till information kontrolleras månadsvis för att säkerställa att de hanteras utan onödigt dröjsmål.

3.5 Säkerställa rätten till rättelse

Syfte:

- Att säkerställa att de registrerade kan få sina uppgifter rättade vid felaktigheter

Riktlinjer:

Vid förfrågan från de registrerade måste företaget rätta all ofullständig eller felaktig information om den berörda personen.

En anställd som mottar en begäran om rättning eller som upptäcker att felaktig information behandlas, måste anmäla detta till den personuppgiftsansvarige som rättar de felaktiga uppgifterna.

Kontroll:

Exempel på kontroll:

Förfrågningar avseende rättelser kontrolleras regelbundet för att säkerställa att de hanteras utan onödigt dröjsmål.

3.6 Gallring och rätten att bli glömd/raderad

Syfte:

- Personuppgifter raderas när det inte längre finns ett syfte med behandlingen
- Att säkerställa att den registrerade har rätt att bli raderad/glömd

Riktlinjer:

I registerförteckningen har angetts gallringstiden för varje behandling.

Personuppgifter lagras på definierade lagringsytor och system för att minimera spridningen av personuppgifter i organisationen och för att underlätta raderings- gallringsprocessen. Om anställda har ett behov av att tillfälligt lagra personuppgifter lokalt, ska dessa raderas så snart arbetet/behovet är avklarat.

Det skall också säkerställas att information gallras/raderas från personuppgiftsbiträden.

Personuppgifter ska regelbundet raderas:

Anställda ska regelbundet radera/gallra e-mail som innehåller personuppgifter när dessa flyttats och lagras på avsedda platser eller när det inte längre finns ett syfte att behandla uppgifterna.

Anställda förstör fysiska dokument som innehåller personuppgifter regelbundet när dessa inte längre behövs.

Den ansvariga för system innehållande personuppgifter raderar eller anonymiserar data i systemen när de inte längre har något syfte eller behövs för behandlingen.

Innan någon information raderas måste det säkerställas att den inte behöver lagras för att uppfylla någon annan regel/ annat lagkrav.

Rätten att bli bortglömd:

När en registrerad begär att bli bortglömd, måste denna begäran vidarebefordras till den personuppgiftsansvarige som raderar detta utan onödigt dröjsmål efter att ha säkerställt att det inte längre finns ett syfte/behov av att behandla informationen. Det måste säkerställas att den registrerade

inte har några utestående/oavslutade affärer/kontrakt med företaget innan informationen raderas. Anställda som hanterar begäran om radering av uppgifter måste underrätta den registrerade om företaget inte helt eller delvis kan uppfylla Kravet om radering t.ex. att det inte är möjligt att fortsätta tillhandahålla en tjänst om man inte har personuppgifterna. Den registrerade måste alltid ha möjligheten att radera uppgifter som är inhämtade med samtycke som laglig grund. Den registrerades identitet ska säkerställas innan uppgifter raderas.

Radering av uppgifter i backuper:

Om behovet uppstår att läsa tillbaka en backup, säkerställs det att raderad information I produktionsmiljön raderas återigen vid återläsning, detta genomförs manuellt.

Kontroll:

Exempel på kontroll:

Gallringstiden på personuppgiftsbehandlingar ses över årligen.

Årligen genomförs controller I CRM systemet för att radera uppgifter om kunder som inte längre ska finnas I systemet.

Kvartalsvis kontrolleras att de raderingar som ska ha genomförts är genomförda.

Regelbundet kontrollerar anställda att personuppgifter som sparats lokalt eller i mail flyttas till avsedd plats och raderas från mailbox och lokal dator.

3.7 Begränsning i behandling av personuppgifter

Syfte:

- Begränsa behandlingen av personuppgifter till att bara omfatta lagring

Riktlinjer:

När en registrerad begär att behandlingen av dennes personuppgifter ska begränsas, ska den personuppgiftsansvarige vid företaget informeras omedelbart. Behandlingen av personuppgifter begränsas då till att endast lagra personuppgifterna intill dess att anledningen till begäran om begränsning av behandlingen är utredd och åtgärdad.

Kontroll:

Exempel på kontroll:

Begäran om begränsning av behandling kontrolleras regelbundet för att tillse att företaget verkligen begränsat behandlingen till att endas omfatta lagring och att detta gjordes utan onödigt dröjsmål.

3.8 Rätten att invända

Syfte:

- Att tillgodose den registrerades rättighet att invända mot profilering och direktmarknadsföring

Riktlinjer:

När en registrerad meddelar att han/hon inte vill att personuppgifter används för profilering eller direktmarknadsföring, kontakta omedelbart företagets personuppgiftsansvarig, så då tillser att behandling av personuppgifter i syfte att profilera eller direktmarknadsföring upphör.

Kontroll:

Exempel på kontroll:

Inkomna begäran om begränsning kontrolleras regelbundet för att tillse att företaget inte längre använder informationen för profilering

3.9 Biträdesavtal

Syfte:

- Att tillse att biträdesavtal finns upprättade med andra som har tillgång till personuppgifter eller som vi skickar personuppgifter till.

Riktlinjer:

Biträdesavtal har ingåtts med alla organisationer som har tillgång till företagets personuppgifter eller som företaget skickar personuppgifter till.

Vid varje tillfälle då ett nytt avtal ingås med en leverantör ska det utvärderas om tjänsten kommer att innebära/innehålla några personuppgifter. Om så är fallet skall ett biträdesavtal upprättas.

Regelbundna kontroller genomförs hos biträden genom att erhålla revisionsunderlag eller genomföra besök hos leverantören för att säkerställa att biträdesavtalet efterlevs.

Biträdesavtal lagras centralt hos den personuppgiftsansvarige vid företaget.

Om en anställd upptäcker eller blir medveten om att behandlingen av personuppgifter hos biträdet inte följer upprättade avtal måste han/hon anmäla detta till den personuppgiftsansvarige vid företaget.

Kontroll:

Exempel på kontroller:

Vid regelbundna tillfällen kontrolleras listan på aktuella biträden och matchas mot aktuella biträdesavtal för att säkerställa att avtalet fortfarande är tillräckligt.

Årligen inhämtas revisionsunderlag från IT leverantörer rörande framförallt behandlingen av personuppgifter för att utvärdera och tillse att biträdesavtal följs.

3.10 Säkerställa dokumentation

Syfte:

- Att möta kraven enligt GDPR på registerförteckning och genomförda riskanalyser.

Riktlinjer:

Företaget har upprättat en registerförteckning som finns hos den personuppgiftsansvarige vid företaget. Förteckningen uppdateras regelbundet då nya behandlingar genomförs eller förändringar sker inom företaget rörande personuppgiftsbehandlingar.

Kontroll:

Exempel på kontroller:

Företagets behandlingar revideras årligen för att avgöra om några högriskbehandlingar genomförs, syftet är också att avgöra om en ny riskanalys och åtgärdsplan behöver upprättas för att minska ev. risker. Om det inte är möjligt att minska risken, måste tillsynsmyndigheten konsulteras innan behandlingen påbörjas. Riskanalyser uppdateras vid planer på nya behandlingar eller ändringar i redan existerande behandlingar.

3.11 Datasäkerhet

Syfte:

- Att säkerställa att nödvändiga organisatoriska och tekniska åtgärder vidtagits för att förebygga att personuppgifter oavsiktligen avslöjas eller förloras.

Riktlinjer: - Begränsning av åtkomst till personuppgifter som lagras elektroniskt.

Alla system/lagringsplatser som innehåller personuppgifter har begränsningar i åtkomst, så att endast anställda som har behov av uppgifterna i sitt arbete har tillgång till dem.

Kontroll:

Exempel på kontroller:

Regelbundet genomförs kontroller på behörigheter till system och lagringsytor för att säkerställa att detta stämmer överens med de arbetsuppgifter de anställda har och att de behöver åtkomst till personuppgifterna.

Riktlinjer: - Epost med personuppgifter

Epost som innehåller personuppgifter ska begränsas till ett absolut minimum, där det fortfarande finns ett behov av att skicka personuppgifter via email ska dessa krypteras och sändas via säker epost.

Kontroll:

Exempel på kontroller:

Generella säkerhetsinställningar i IT-miljön kontrolleras regelbundet

3.12 Fysisk säkerhet

Syfte:

- Att säkerställa att åtgärder vidtagits för att förhindra att obehöriga får tillgång till platser där behandling av personuppgifter sker.

Riktlinjer:

Områden där behandling av personuppgifter behandlas säkras så att obehöriga inte kan få tillgång till dem. Detta uppnås genom att lagra personuppgifter I låsta skåp/lådor när rummet lämnas obevakat. Vidare arkiveras regelbundet personuppgifter i låsta arkivrum.

Alla anställda ska låsa sin dator genom skärmlås så snart datorn lämnas, även om det bara är för en kort stund. På företaget gäller också clean desk policy, som innebär att alla anställda ska lägga undan/låsa in dokument när arbetsplatsen lämnas. De anställda ska även tillämpa sk. Front down policy, vilket innebär att dokument innehållande personuppgifter ska vändas upp och ner eller täckas över när arbetsplatsen lämnas.

För mer information kring säkerhet hänvisas till företagets IT- och informationssäkerhetspolicy.

Kontroll:

Exempel på kontroll:

Genomgång av dokument i låsta skåp skall genomföras årligen.

Slumpvisa kontroller ska genomföras för att säkerställa att skåp och lådor halls låsta och att endast de anställda som ansvarar för skåpet/lådan har nyckel

Kontroller och påminnelser ska ske så att anställda verkligen låser sina datorer när de lämnar arbetsplatsen.

3.13 Utskrifter och dokument med personuppgifter

Syfte:

- Personuppgifter i pappersform ska hanteras på rätt sätt.

Riktlinjer:

Säkerställ att utskrifter övervakas om du skriver ut dokument som innehåller personuppgifter och låt inte dokument som innehåller personuppgifter bli liggande i skrivaren.

Lämna inte pappersdokument som innehåller personuppgifter obevakade på arbetsplatsen.

Alla fysiska dokument (brev, utskrivna email, anteckningar m.m.) som innehåller personuppgifter skall förstöras i därför avsedd återvinning alternativt förstöras i dokumentförstörare.

Kontroll:

Exempel på kontroll:

Regelbundna kontroller ska ske för att säkerställa att det inte ligger kvar dokument i skrivare som innehåller personuppgifter och att det inte lämnas dokument innehållande personuppgifter obevakat på arbetsplatserna.

3.14 Utbildning och kunskap hos anställda

Syfte:

- Att säkerställa att samtliga anställda är medvetna om de krav och regler som gäller kring hantering av personuppgifter

Riktlinjer:

Alla anställda vid TiksPac skall underteckna ett sekretessavtal i samband med anställning.

Alla nyanställda måste utbildas i de regler och riktlinjer som gäller för hantering av personuppgifter i samband med deras anställning.

Kontroll:

Exempel på kontroll:

I samband med anställning skriver den anställde under sekretessavtalet och att hen läst och förstått företagets personuppgiftspolicy.

Årligen ska samtliga anställda delta i utbildning rörande behandling av personuppgifter.

3.15 Rapportering av personuppgiftsincident

Syfte:

- Att säkerställa att tillsynsmyndigheten meddelas inom 72 timmar samt vid särskilda fall även de drabbade så snart som möjligt.

Riktlinjer:

Incident definieras som en händelse som riskerar att personuppgifter görs tillgängliga för personer som inte är behöriga att ta del av dessa eller att personuppgifter förloras eller förstörs.

Om en anställd upptäcker en incident eller ett brott mot säkerheten, måste detta snarast rapporteras till den personuppgiftsansvarige vid företaget som tillsammans med de berörda anställda samlar in information om incidenten, mängden personuppgifter och mängden berörda registrerade, eventuella konsekvenser för de registrerade och sedan avgör om en rapport till tillsynsmyndigheten ska ske

Om incidenten är så allvarlig att de registrerade måste meddelas skall detta göras via email.

För information kring hur företaget skyddar personuppgifter och upptäcker eventuella incidenter, hänvisas till företagets IT- och informationssäkerhetspolicy.

Kontroll:

Exempel på kontroll:

Det genomförs regelbundet kontroller på att situationer som ska meddelas tillsynsmyndigheten också rapporteras inom 72 timmar.

3.16 Privacy by Design och Privacy by Default

Syfte:

- Att efterleva förordningens krav på Privacy by design och Privacy by default

Riktlinjer:

Vid inköp eller utveckling av nya IT-system ska företaget säkerställa att systemen är säkra och att de uppfyller kraven på skydd av personuppgifter, separation av användare och skydd mot förlust av data.

Anställda får inte använda tjänster som behandlar personuppgifter utan att detta har godkänts av den personuppgiftsansvarige eller IT-ansvarige vid företaget, detta gäller även privata email klienter, privata molntjänster som kan laddas ner från internet.

Kontroll:

IT-avdelningen har checklistor kring hur nya system och tjänster får utvecklas/anslutas till befintliga system. IT-avdelningen genomför regelbundna kontroller på vilka system som används och söker även av nätverket för att säkerställa att inte obehöriga program används.

4. Cookies

När man besöker vår hemsida samlas information om besökaren in, detta görs i syfte att säkerställa att besökaren får den bästa upplevelsen av hemsidan med tillgång till alla funktioner. För att kunna använda vår webbplats på det sätt vi avsett rekommenderar vi därför att man tillåter lagring av cookies på sin dator. Om du inte tillåter cookies riskerar man att få en sämre användarupplevelse och att inte kunna använda webbplatsen till fullo.

Det finns två typer av cookies. Den ena typen sparar en fil under en längre tid på datorn. Den används till exempel vid funktioner som talar om vad som är nytt sedan användaren senast besökte den aktuella webbplatsen. Den andra typen av cookies kallas sessionscookies. Under tiden man är inne och surfar på en sida, lagras den här cookien temporärt i datorns minne, exempelvis för att hålla reda på vilket språk som valts. Sessionscookies lagras inte under en längre tid utan försvinner när webbläsaren stängs ned. Cookies kan inte innehålla skadligt innehåll såsom till exempel virus.

Om man inte vill att information samlas in är det möjligt att radera eller blockera cookies i webbläsarens inställningar.