Lathund
Dataskydd för krögare

General Data Protection Regulation (GDPR), eller dataskyddsförordningen på svenska, ersätter Personuppgiftslagen och ska börja tillämpas den 25 maj 2018. Den kan verka skrämmande, framför allt med tanke på de höga ”bötesbeloppen” som ett företag kan drabbas av om de inte följer GDPR. Men egentligen handlar GDPR om att ha kontroll över behandlingen av personuppgifter och ha ordning och reda i systemen.

BEHANDLING AV PERSONUPPGIFTER

Om ni har ett kundregister, ett löne- eller personalregister, eller om ert företag i andra sammanhang samlar in och/eller lagrar personuppgifter, dvs. uppgifter om namn, personnummer, e-postadresser, bilder eller andra uppgifter som gör det möjligt att identifiera en fysisk person – då behandlar ni personuppgifter.

TÄNK ATT NI BARA LÅNAR UPPGIFTERNA

Grundtanken om personuppgifter är att ni bara lånar personuppgifterna från en person för att kunna uppfylla ett syfte i din verksamhet. Tänk er att ni lånar porslin från en annan restaurang för att kunna servera en extra stor middag. Ni skulle antagligen:

- Bara använda porslinet till just den middagen som ni lånat det för
- Bara låna exakt så mycket porslin som behövs
- Vara extra försiktiga med porslinet så att det inte försvinner eller går sönder
- Lämna tillbaka det så fort middagen var över

På samma sätt ska ni tänka när ni behandlar personuppgifter i er verksamhet, vare sig det handlar om era anställda eller era kunder. Se till att personuppgifterna bara används för det syfte som ni samlat in dem för, skydda dem från obehöriga, ha kontroll på hur och varför de används, informera om vad ni gör med personuppgifterna och lämna tillbaka dem när ni inte längre behöver dem.

NI BEHÖVER OCKSÅ SE TILL ATT DET FINNS EN RÄTTSLIG GRUND FÖR ATT KUNNA BEHANDLA PERSONUPPGIFTERNA:

- Fullgörande av avtal kan användas som grund för att till exempel behandla personuppgifterna för era anställda för att betala ut lön, ha tidrapportering och sätta upp login till systemen som ni använder i verksamheten.
- Rättslig förpliktelse är när det finns en reglering som tvingar er att behandla personuppgifterna. Den här grunden kan till exempel användas för att innehålla preliminärskatt och rapportera till Skatteverket och Försäkringskassan.
- Berättigat intresse handlar om att göra en intresseavvägning mellan hur viktigt det är för er verksamhet att få behandla personuppgifterna kontra personens integritet. Ni måste alltså objektivt kunna motivera varför ert intresse väger tyngre än personens integritet.
- Samtycke kan användas för att spara uppgifter om gästernas allergier eller dra fackföreningsavgiften direkt från den anställdes lön. GDPR ställer höga krav på hur ett samtycke inhämtas för att det ska vara giltigt, så kan ni stödja behandlingen på någon av de andra grunderna är det att föredra.

Om det är fråga om uppgifter om hälsa (t.ex. sjukfrånvaro), ras, etniskt ursprung, fackföreningstillhörighet, politiska åsikter, uppgifter om sexuell läggning eller sexualliv, biometriska och genetiska uppgifter eller religiös tro (så kallade känsliga personuppgifter) ställs särskilda krav, såsom uttryckligt samtycke eller lagstöd. Det **krävs** dessutom högre IT-säkerhet.

Ni måste alltså ta kontroll över hur och när personuppgifterna behandlas. Att exempelvis i ett register över restaurangens anställda ha noterat en persons sexuella läggning, etniska ursprung, vissa uppgifter om hälsa eller annat som inte är direkt nödvändigt för att uppfylla anställningsavtalet, är normalt sett inte förenligt GDPR. Lönekontoret har inget intresse av att veta att Rickard är allergisk mot jordnötter, och hovmästaren har inget intresse av att veta att Rickard stämplade in två minuter senare än Emma.

Vad gäller era gäster ska ni helt enkelt använda sunt förnuft. Det finns ingen rättslig grund att notera att Rickard snålade med dricksen. Det kan däremot vara en bra idé att notera hur många i sällskapet som är vegetarianer eller önskar alkoholfria alternativ. Bokar era kunder bord hos er får ni behandla gästens personuppgifter för bordsbokningen baserat på den rättsliga grunden berättigat intresse.

Vill ni skicka ut marknadsföringsmail till de kunder som bokat bord och därmed lämnat sin mailadress till er, är det okej så länge som ni har informerat om att detta kommer ske när de bokade bordet och därmed lämnade sin mailadress. Det är alltså viktigt att ge rätt och tillräcklig information till de som lämnar personuppgifter till er, och informationsplikten gäller både för era gäster och era anställda.

Personen som uppgifterna handlar om har fått utökade rättigheter i GDPR. Bland annat har vem som helst som finns i era system (både gäster och anställda) rätt att begära ut en kopia på samtliga uppgifter som ni har om han och uppgifterna ska skickas till personen inom en månad. För att det ska vara praktiskt möjligt krävs det alltså att det är ordning och reda i systemen så att ni vet var ni ska leta fram uppgifterna. Förutom rätten att begära ut kopia kan personen också hävda sin ”rätt att bli glömd”, vilket i praktiken betyder att ni ska radera alla uppgifter som finns om hen i systemen. Rätten att bli glömd trumfar dock inte om någon lag som t.ex. bokföringslagen tvingar er att ha kvar uppgifterna, eller om gästen har en utestående faktura att betala, då är det tillåtet att ha kvar uppgifter för att uppfylla kraven.

RELATIONEN MELLAN CASPECO OCH RESTAURANGER

När ni i er restaurangverksamhet använder Caspecos tjänster är ni (den juridiska personen) personuppgiftsansvarig och Caspeco personuppgiftsbiträde. Även om det är Caspeco som tillhandahåller tid-och lönesystem, bokningssystem osv så är det restaurangverksamheten som betraktas vara personuppgiftsansvarig eftersom det i slutändan är restaurangverksamheten som bestämmer ändamålen och medlen för behandlingen av personuppgifter. Du hade alltså kunnat ha Rickard som anställd och Emma som kund – oavsett om du använder Caspeco eller ett konkurrerande system. Personuppgiftsbiträdet är den som behandlar personuppgifter för personuppgiftsansvariges räkning, dvs. Caspeco behandlar bara personuppgifter åt er på instruktioner av er.

GDPR ställer nya krav på personuppgiftsbiträden och Caspeco jobbar aktivt för att plattformar och andra processer som behandlar personuppgifter ska vara förenliga med förordningen. Bland annat finns det krav på ett skriftligt avtal mellan den personuppgiftsansvariga och personuppgiftsbiträdet och skyldighet att se till att det finns ligger hos båda. Caspeco kommer dock inom kort skicka ut uppdaterade så kallade personuppgiftsbiträdesavtal, där bland annat er respektive Caspecos roll regleras. Caspeco kontrollerar löpande samtliga underleverantörer, dvs. underbiträden och tecknar underbiträdesavtal med dessa. Ett underbiträdesavtal omfattas av samma skyldigheter som personuppgiftsbiträdet har gentemot den personuppgiftsansvarige. Om ett underbiträde inte fullgör sina skyldigheter ställs personuppgiftsbiträdet fullt ansvarig mot personuppgiftsansvarige.

ÖVRIGA NYHETER SOM KAN PÅVERKA DIG SOM RESTAURANGÄGARE

Utöver strängare krav på personuppgiftsbiträdet införs med GDPR andra nyheter som kan vara nyttiga för dig som restaurangägare att känna till.

MISSBRUKSREGELN

Först och främst försvinner den så kallade missbruksregeln. Missbruksregeln innebär lättare rättsliga förhållande för behandling av personuppgifter i e-post, på webbplatsen eller i enkla listor som man har i datorn. När missbruksregeln försvinner innebär det att samma regler som gäller för behandling av personuppgifter i bokningssystem och kundregister också gäller för det som skrivs om personer i exempelvis e-post och på webbplatser. Innebörden av detta blir därför att bestämma rättslig grund för behandlingen, att informera berörda personer och föra register över sina behandlingar. Att ladda upp bilder på anställda kommer alltså att kräva mer än vad det gör med personuppgiftslagen.

PERSONUPPGIFTSINCIDENT

Om det är så att restaurangen råkar ut för oavsiktlig eller olaglig förstöring, förlust eller ändring, obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlas inom verksamheten, ska detta inom 72 timmar meddelas tillsynsmyndighet (Datainspektionen).

DATASKYDD SOM STANDARD

Personuppgiftsbiträde och personuppgiftsansvariga ska vidta lämpliga åtgärder för att uppfylla kraven i GDPR. Med lämpliga åtgärder menas att ställa tekniska och organisatoriska åtgärder mot personuppgifternas art, i vilken omfattning personuppgifter behandlas samt den risk som individen utsätts för vid behandling.

SANKTIONSAVGIFT

Datainspektionen ges rätt att utdöma en sanktionsavgift för den som bryter mot dataskyddsförordningen. Vid beräkning ska beaktas hur allvarlig överträdelsen är.

DATASKYDDSOMBUD

GDPR kräver att tre typer av organisationer ska utse ett så kallat dataskyddsombud, dvs en roll som har särskilt ansvar för dataskydd i organisationen. Det krävs för en organisation som är offentligt organ eller myndighet, där kärnverksamheten kräver regelbunden och systematisk övervakning i stor omfattning eller där kärnverksamheten behandlar känsliga personuppgifter (såsom hälsa, facklig tillhörighet eller religion) eller fällande domar i brottmål i stor omfattning.

CHECKLISTA, DATASKYDD FÖR KRÖGARE

- Se till att ni har en rättslig grund för behandlingen av personuppgifter. Tänk på att inte skriva kränkande kommentarer i kundregistret, eller kommentarer som inte är nödvändiga för ändamålet med kundregistret.
- Samla aldrig in mer personuppgifter än vad som är nödvändigt för ändamålet. Skilj på personuppgifter som samlas in för att de behövs och de personuppgifter som är bra att ha (need vs. nice). Ni ska bara behandla de uppgifter som ni behöver!
- Spara aldrig personuppgifter längre än vad som är nödvändigt för ändamålet. Vad som är nödvändigt beror helt på vilket ändamål som de behandlas för. Caspeco kommer att hjälpa er att sätta rutiner för när vissa personuppgifter ska tas bort ur systemen, men ansvaret för detta ligger ändå hos den personuppgiftsansvariga, dvs er.
- För register över behandling som utförts under ert ansvar. Ett sådant register ska innehålla följande uppgifter:
- Restaurangverksamhetens (personuppgiftsansvarig) namn och kontaktuppgifter.
- Ändamålet med behandlingen.
- En beskrivning av kategorierna av registrerade (anställda, kunder, kontaktpersoner osv) och av kategorierna av personuppgifter (namn, adressuppgifter, telefonnummer osv).
- De kategorier av mottagare (lönekontor, samarbetspartners osv) till vilka personuppgifterna har lämnats eller ska lämnas ut. Detta kan exempelvis vara Caspeco.
- Om möjligt, den bestämda tiden för hur länge uppgifterna kommer att sparas.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder. Detta kan exempelvis vara att lönekontoret inte har tillgång till vissa uppgifter som HR har, och tvärtom.
- Införliva och följ sådana organisatoriska åtgärder som nämns i 4.g ovan. Behörighetsåtgärder är ett enkelt sätt att skydda personuppgifter från obehöriga. En huvudregel är att behörighet till personuppgifter bara ska lämnas till de som behöver åtkomst för att kunna utföra sitt arbete.
- Om verksamheten har för avsikt att ladda upp bilder eller kommentarer från nöjda anställd eller gäster, glöm inte att först fråga!
- Informera era anställda och gäster hur ni behandlar deras personuppgifter! Ladda t.ex. upp er informationstext på er webbsida och lägg in det i personalhandboken.