			Datum	Upprättat av:	
			2018-09-27	HR-chef	
Fastställd av:	Status:	Revision:	Rev.datum:	Dokumentnr:	Ärendenr:
Styrelsen	FASTSTÄLLD	1.1	2022-05-19		

Ämne:

Dataskyddspolicy

1 Syfte och omfattning

Kaunis Iron-koncernen (Kaunis Iron) har i egenskap av personuppgiftsansvarig att hantera personuppgifter i enlighet med gällande dataskyddslagstiftning. För att säkerställa korrekta rutiner och efterlevnad av lagstiftningen har Kaunis Iron antagit denna dataskyddspolicy (”Policyn”). I sin roll som personuppgiftsansvarig är det Kaunis Irons ansvar att säkerställa de personuppgifter som Kaunis Iron behandlar. Policyn omfattar samtliga anställda vid Kaunis Iron inklusive leverantörer som utför arbete för Kaunis Irons räkning. Alla som omfattas av Policyn har ett personligt ansvar för att gällande dataskyddslagstiftning och Policyn efterlevs. Härutöver har Kaunis Iron ett s.k. dataskyddsombud som ska säkerställa denna efterlevnad och att det finns en medvetenhet om dataskydd inom Kaunis Iron (se punkt 14 nedan).

Policyn omfattar hela koncernen inklusive dess moder- och dotterbolag.

2 Definitioner

I Policyn tillämpas följande definitioner.

Automatiska data

Information på en dator eller information som ska/kommer behandlas på en dator. Omfattar inte endast databaser/register utan även t.ex. e-post, dokument och övervakningsbilder.

Behandling

Alla former av åtgärder som inkluderar en personuppgift, till exempel insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, användning, utlämning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Data

Information som kan behandlas, såväl automatiskt som manuellt. Dataskyddsombud Den av Kaunis Iron utsedda personen med ansvar för att Kaunis Iron efterlever relevant lagstiftning, se punkt 14 nedan.

GDPR

EU:s dataskyddsförordning (”GDPR”) - Förordning 2016/679 som träder i kraft i maj 2018 och ersätter det nuvarande dataskyddsdirektivet 95/46/EG och den svenska personuppgiftslagen (PuL).

Känsliga personuppgifter

Personuppgifter som rör en persons etnicitet, politiska åsikter, fackmedlemskap eller religiösa eller andra övertygelser, fysisk eller psykisk hälsa, sexuell läggning, brottmålsdomar eller anmälningar om påstådda brott.

Manuell data

Information som hålls som en del av ett arkiveringssystem, eller med avsikt att det ska ingå i ett arkivsystem, inkluderande tillfälliga mappar.

Personuppgiftsansvarig

En person eller ett företag som (ensam eller med andra) kontrollerar innehållet och användningen av personuppgifter.

Personuppgiftsbiträde

En person eller ett företag utanför den personuppgiftsansvariges organisation som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige (t.ex. molntjänstleverantör, revisionsbyrå m.m.).

Registrerad

En registrerad är en person vars personuppgifter behandlas av Kaunis Iron eller bearbetas av ett personuppgiftsbiträde.

Personuppgift

Alla uppgifter som kan knytas till en nu levande, identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Typiska personuppgifter är personnummer, namn och adress. Bilder på och ljudupptagningar av individer som behandlas i dator kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis ip-nummer och cookies, räknas som personuppgifter om de kan kopplas till fysiska personer. Även information som har kodats, krypterats eller pseudonymiserats men som kan hänföras till en fysisk person med hjälp av kompletterande uppgifter är personuppgifter.

3 Principer för behandling av personuppgifter

3.1 Övergripande principer

Kaunis Iron ska i all sin behandling av personuppgifter tillämpa följande principer:

3.1.1 Laglig insamling och behandling

Insamlingen och behandlingen ska ske rättvist och i enlighet med gällande dataskyddslagstiftning. All insamling av information ska ske utifrån ett tydligt behov och en rättslig grund.

Med rättslig grund menas:

- att den registrerade lämnat samtycke till behandlingen,
- att det finns ett avtal mellan Kaunis Iron och den registrerade vilket innebär att viss behandling av personuppgifter måste ske,
- att det föreligger en rättslig förpliktelse som kräver behandling av personuppgifter (t.ex. domstolsbeslut eller bokföringsskyldighet enligt bokföringslagen),
- att skydda den registrerades grundläggande intressen (t.ex. skydda dennes eller annans hälsa),
- att utföra en uppgift av allmänt intresse (t.ex. myndighetsutövning), eller
- intresseavvägning (behandlingen är nödvändig och Kaunis Iron intresse väger tyngre än den registrerades integritetsskydd, t.ex. viss marknadsföring).

Kaunis Iron behandlar endast personuppgifter utifrån ett specifikt, tydligt och lagligt ändamål. Det är således olagligt att insamla personuppgifter rutinmässigt och utan ett tydligt och lagligt syfte. Det får inte ske någon behandling utifrån att personuppgifterna kan bli relevanta i framtiden. När behandlingen sker utifrån ett särskilt ändamål, får personuppgifterna inte behandlas för något annat ändamål än det för vilket personuppgifterna erhölls. Uppgifter om personuppgifter som behandlas av Kaunis Iron finns i särskilt/särskilda personuppgiftsregister.

3.1.2 Transparens

Den registrerade måste informeras om hur dennes personuppgifter hanteras. När uppgifterna samlas in, ska den registrerade informeras om bl.a. ändamålet med behandlingen, vilka rättigheter den registrerade har och hur behandlingen sker.

3.1.3 Säker behandling

Kaunis Iron använder sig av lämpliga säkerhetsåtgärder mot obehörig tillgång eller förändring, avslöjande, förstörelse eller olaglig behandling av personuppgifter och mot oavsiktlig förlust eller förstörelse av sådan data. Anställdas tillgång till de

personuppgifter som behandlas av Kaunis Iron är begränsad till en ”need to know basis”

3.1.4 Korrekta och aktuella personuppgifter

Kaunis Iron ska säkerställa att de personuppgifter som behandlas är korrekta, fullständiga och uppdaterade. Felaktigheter kommer rättas så snart det är möjligt

3.1.5 Gallring

Personuppgifter ska inte sparas längre än vad som är nödvändigt utifrån ändamålet med behandlingen. Personuppgifter får inte sparas på obestämd tid.

3.1.6 Rätt till tillgång till personuppgifter

Registrerade har rätt till information och tillgång till den behandling som rör dem. Se närmare information om detta under punkt 8 nedan.

3.2 Samtycke

Ett samtycke innebär att den registrerade lämnar sitt samtycke till viss personuppgiftsbehandling. Samtycket ska vara frivilligt (muntligt eller skriftligt) och lämnas efter att den registrerade fått information om personuppgiftsbehandlingen. Om ett muntligt samtycke mottas bör mottagandet noteras skriftligen i aktuellt ärende. Det bör övervägas om någon annan rättslig grund, se 3.1, är tillämplig eftersom ett lämnat samtycke kan återkallas. E-postkonversationer, kontaktuppgifter till en potentiell kund, nyttjande av digitala tjänster/platser eller CV från arbetssökanden är exempel då samtycke är lämpligt för personuppgiftsbehandling. Särskilt höga krav gäller när samtycke avser behandling av känsliga personuppgifter. Den som behandlar personuppgifter med stöd av ett samtycke måste kunna visa att ett giltigt samtycke har lämnats av den registrerade.

3.3 Personuppgift som behandlas innan den 25 maj 2018

De uppgifter som behandlats före den 25 maj 2018 anses ha behandlats korrekt om de har behandlats i enlighet med den tidigare personuppgiftslagen. Behandlas dessa uppgifter även den 25 maj 2018 och därefter, ska uppgifterna behandlas i enlighet med GDPR och Policyn.

4 Principer för användning av mobiltelefoner, datorer m.m

Kaunis Iron tillhandahåller datorer, mobiltelefoner och andra tekniska medel i syfte att de anställda ska kunna utföra sina arbetsuppgifter. Användandet av dessa hjälpmedel ska i alla avseenden ske med beaktande av GDPR och Policyn,

vilket exempelvis innebär att nyttjandet ska ske på ett sådant sätt att risk för obehörig behandling av personuppgifter minimeras. Alla tekniska hjälpmedel ska förses med lösenord som endast den anställde har tillgång till. Alla tekniska hjälpmedel ska ha den programvara och de övriga applikationer som tillhandahållits av Kaunis Iron. Vid behov av annan programvara eller kompletterande installation ska anmälan ske till IT-ansvarig samt till dataskyddsombudet. Vid eventuell stöld eller annan förlust av tekniskt hjälpmedel ska anmälan omgående lämnas till närmsta chef samt till dataskyddsombudet.

Se även riktlinjer för mobil- och dataanvändning.

5 E-post

E-post ska hanteras i enlighet med GDPR och Policyn. Det innebär att det krävs en laglig grund (samtycke, avtal etc.) för att lagra eller processa personuppgifter genom e-post. Om en e-postkonversation behandlar en fråga som är nödvändig för att uppfylla ett avtal mellan en part och Kaunis Iron behövs inget ytterligare samtycke. När avtalsförhållandet har upphört ska personuppgifterna gallras bort, förutsatt att inte finns någon laglig grund för att spara personuppgifterna, t.ex. som underlag för bokföring (lagkrav), alternativt om tvister eller liknande kan uppkomma i efterhand för vilka e-postkonversationen kan få betydelse som bevismedel.

För att underlätta hanteringen av samtycke och gallring bör e-post endast användas som transportör av personuppgifter, dvs. inte för t.ex. lagring eller process (eg. ”master”) av vital information (på detta sätt kan e-post gallras utan att vital information går förlorad). Eftersträva att ha endast ett ärende per e-postkonversation. Undvik massutskick och att – i den mån det är möjligt - skicka personuppgifter via e-post. När man tar emot ett meddelande kan man ha som utgångspunkt att den som skickade meddelandet gav samtycke till just det specifika meddelandet. Det är dock viktigt att man lämnar information om Kaunis Irons personuppgiftsbehandling till den som skickat meddelandet t.ex. genom länk till Kaunis Irons integritetsskyddspolicy i e-postsignaturen. När man skickar e-post finns det alltid en risk att andra än den avsedda mottagaren kan ta del av meddelandet. Om man ska skicka ett e-postmeddelande med personuppgifter som är av ”okänslig” natur och tål andras ögon behöver man normalt sett inte vidta några extra säkerhetsåtgärder. Det kan räcka med de åtgärder man vanligen använder för att skydda sin information, t.ex. brandväggar och virusskydd. Om e-posten däremot innehåller integritetskänsliga personuppgifter måste man ofta vidta särskilda säkerhetsåtgärder, till exempel kryptering. Av GDPR följer att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Nivån på säkerheten ska anpassas till:

- vilka integritetsrisker behandlingen medför,
- hur känsliga de behandlade personuppgifterna är
- vilka tekniska möjligheter som finns
- vad det kostar att genomföra åtgärderna.

6 Överföring av personuppgifter till en tredje part

Kaunis Iron kommer inte att dela registrerades personuppgifter med tredje part annat än när (i) det är specifikt avtalat mellan Kaunis Iron och den registrerade, (ii) när det är nödvändigt för att tillvarata den registrerades rättigheter, (iii) om det följer av lagstadgad skyldighet, myndighetsbeslut eller domstolsbeslut eller (iv) om Kaunis Iron anlitar oberoende leverantörer för tjänster i anslutning till Kaunis Iron verksamhet. Dessa leverantörer kan hantera personuppgifter och behöver ibland begränsad tillgång till personuppgifter som är insamlade av Kaunis Iron. Kaunis Iron kommer alltid att sträva efter att begränsa sådan tillgång till personuppgifter och endast dela information som skäligen behövs för att leverantörerna ska kunna göra sitt arbete eller tillhandahålla sina tjänster. Kaunis Iron kommer även kräva av dessa leverantörer att de (i) skyddar personuppgifter i enlighet med Policyn och (ii) inte använder eller avslöjar personuppgifter i något annat syfte än att tillhandahålla Kaunis Iron avtalade produkter eller tjänster. Personuppgifter kommer inte lämnas ut till tredje part för marknadsföringsändamål utan den registrerades skriftliga samtycke. Kaunis Iron kommer inte att föra över personuppgifter till tredje land (dvs. ett land utanför EU/EES) utan den registrerades skriftliga samtycke.

7 Personuppgiftsbiträde

Personuppgiftsbiträde (”Biträdet”) är den som behandlar personuppgifter för Kaunis Irons räkning. Biträdet finns alltid utanför Kaunis Irons organisation. Biträdet kan vara en fysisk person eller ett företag, offentlig myndighet, institution eller annat organ. Kaunis Iron och Biträdet måste upprätta ett så kallat personuppgiftsbiträdesavtal (”PUBA”) i enlighet med gällande dataskyddslagstiftning. Om en anställd inom Kaunis Iron ger någon utanför företaget tillgång till personuppgifter i syfte att denne ska behandla personuppgifterna för Kaunis Irons räkning ska dataskyddsombudet först informeras i syfte att ett PUBA ska kunna upprättas. Biträden som Kaunis Iron anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i gällande dataskyddslagstiftning och säkerställer att den registrerades rättigheter skyddas. Biträdet och dess personal får enbart behandla

personuppgifter enligt instruktion från Kaunis Iron. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av Kaunis Iron. Biträdet ska föra register över behandlingar och säkerställa en lämplig säkerhetsnivå. Biträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig.

8 Kaunis Iron som personuppgiftsansvarig /personuppgiftsbiträde

8.1 Personuppgiftsansvarig

Kaunis Iron är personuppgiftsansvarig när Kaunis Iron behandlar personuppgifter i sin verksamhet. Kaunis Iron bestämmer då vilka uppgifter som ska behandlas och vad de ska användas till, t.ex. uppgifter om anställda vid Kaunis Iron och uppgifter om Kaunis Irons kunder.

8.2 Personuppgiftsbiträde

Kaunis Iron är normalt sett inte ett personuppgiftsbiträde

9 Registrerades rättigheter

Genom GDPR förstärks de registrerades rättigheter. Några av de viktigaste rättigheterna är:

- rätt till information om behandlingen
- rätt att få tillgång till sina personuppgifter
- rätt att få felaktiga uppgifter rättade
- rätt att få sina personuppgifter raderade
- rätt att invända mot att personuppgifterna används
- rätt till begränsning av behandling
- rättigheter kopplade till automatiserat beslutsfattande och profilering
- rätt att få ut/överföra personuppgifter i maskinläsbart format (dataportabilitet)

Mer information kring de registrerades rättigheter finns på Datainspektionens hemsida, se länk nedan:

http://www.datainspektionen.se/dataskyddsreformen/dataskydds-forordningen/deregistrerades-rattigheter/

10 Begäran om tillgång

Registrerades begäran om tillgång till behandlingen av personuppgifter ska skriftligen ställas till dataskyddsombudet. Efter att dataskyddsombudet mottagit begäran, ska denne granska begäran och bedöma om begäran ska beviljas till hela eller delar samt verkställa beslutet. Dataskyddsombudet ska inom tio arbetsdagar från det att begäran inkom, lämna svar/beslut till den som begär tillgång till information.

11 Sekretess

Personuppgifter är föremål för sekretess. Anställda får bara ha tillgång till personuppgifter som är nödvändiga utifrån ändamålet och omfattningen av den aktuella arbetsuppgiften. All annan behandling av personuppgifter sker obehörigen och är förbjuden. Anställda och leverantörer är förbjudna att använda personuppgifter för privat eller kommersiellt ändamål, eller att göra den tillgänglig på något annat sätt. Sekretessen för personuppgifter för vilka Kaunis Iron är personuppgiftsansvarig kvarstår även efter att anställningen eller uppdraget har upphört.

12 Säkerhet

Lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda personuppgifter, oavsett om personuppgifter behandlas elektroniskt eller i pappersform. Dessa åtgärder måste baseras på den senaste tekniken, riskerna med bearbetning och behovet av att skydda data (informationsklassificering).

13 Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som Kaunis Iron behandlar. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna. Incidenter kan betraktas som små (incidenter som faktiskt inte leder till avslöjanden, förluster m.m.) eller stora (intrång i IT-system, inbrott, stöld av dator m.m.). Incidenter kan uppstå av olika skäl, t.ex. stöld av information/utrustning, obehörig tillgång, fel i utrustning/system, mänskliga fel, hackerattack, brand, felsänd e-post och olämpligt avslöjande av information. Alla personuppgiftsincidenter (även misstänkta personuppgiftsincidenter) ska utan dröjsmål

anmälas till dataskyddsombudet. Dataskyddsombudet har därefter till uppgift att bedöma incidenten och anmälan den.

Informationen i anmälan ska innehålla uppgifter om:

- Vilken typ av incident det är fråga om,
- Vilka kategorier av personer som kan komma att beröras,
- Hur många personer det berör,
- Vilka konsekvenser incidenten kan få, samt
- Vilka åtgärder man vidtagit för att motverka ev. negativa konsekvenser.

Varje incident ska sammanfattas och lagras av Kaunis Iron dataskyddsombud.

14 Dataskyddsombud och kontaktuppgifter

Ombudet ska vara kvalificerad för uppdraget samt känna till lagstiftning och praxis avseende dataskydd. Det får inte föreligga motstående intressen, vilket innebär att dataskyddsombudet normalt behöver vara en annan person än exempelvis VD. Det är av vikt att ombudet kan utföra sitt uppdrag självständigt och oberoende.

Dataskyddsombudets uppgifter kan variera mellan olika verksamhetsområden. Sammanfattningsvis består de obligatoriska uppgifterna av att:

- Informera och ge råd i frågor rörande personuppgiftsbehandling.
- Övervaka efterlevnaden av dataskyddslagstiftningen och Policyn samt tillse att Policyn uppdateras vid behov.
- Fungera som kontaktlänk mellan Datainspektionen, de registrerade samt internt inom Kaunis Iron.

Det är alltid Kaunis Iron (den personuppgiftsansvarige) som bär ansvaret för att dataskyddslagstiftningen efterlevs, även om kontrollen av Kaunis Irons efterlevnad delegeras till ett dataskyddsombud.

Kaunis Irons dataskyddsombud samt kontaktuppgifter till denne framgår nedan.

Dataskyddsombud:	Sara Stridsman
Telefonnummer:	070 – 261 00 77
E-postadress:	sara.stridsman@kaunisiron.se

Denna policy är ett komplement till GDPR och annan gällande dataskyddslagstiftning. Gällande dataskyddslagstiftning har företräde framför Policyn i händelse av

att någon del av Policyn skulle strida mot gällande dataskyddslagstiftning, eller i det fall gällande dataskyddslagstiftning har strängare krav än Policyn.

15 Versionshistorik

Version	Datum	Ändring
1.0	2018-09-27	Första utgåva
1.1	2022-05-19	Ny mall, versionshistorik