General Data Protection Regulation

Detta är IAB Sveriges checklista för våra medlemmar gällande GDPR eller Dataskyddsförordningen och bygger på information från IAB UK och IAB Europe. IAB Sverige och vår moderorganisation IAB Europe arbetar kontinuerligt med att utbilda, informera och tyda vår nya Dataskyddsförordning som ska vara implementerad maj 2018.

Medvetenhet

GDPR (General Data Protection Regulation) eller på svenska: "Allmänna Dataskyddsförordningen", innehåller stora sanktioner- upp till 4% av årlig global omsättning. Men det här är inte den enda anledningen ledningen måste vara medvetna om den nya lagen. En del processer och produkter måste ändras som ett resultat av GDPR. Många digitala annonsörer har kanske inte tidigare gjort en heltäckande genomgång av hur de följer personuppgiftsreglerna.

Vi rekommenderar att du samlar företagets olika avdelningar för att väcka medvetenhet om hur det påverkar alla aspekter av organisationen och skapar en plan för hur man ska uppfylla GDPR genom att involvera personal från alla relevanta avdelningar. Glöm inte bort att GDPR kommer gälla alla företag som är aktiva inom EU så se till att dina kollegor utomlands, även de i USA, är involverade och insatta.

Dokumentera hur ni anpassar er regelefterlevnad

Ansvarsskyldighet är ett centralt tema som genomsyrar GDPR. Grundläggande för att uppfylla ansvarsskyldigheten är att du dokumenterar vilken slags personuppgifter organisationen behandlar och identifiera potentiella risker. Det är något du kan börja med nu. Kom ihåg att definitionen av personuppgifter i GDPR är mycket omfattande. Detta är viktigt att identifiera eftersom ett flertal datapunkter som många i branschen för närvarande anser faller utanför nuvarande dataskyddsdirektiv faktiskt ingår i GDPR. Det betyder att du inte ska anta att unika identifierare (tex cookies eller annons IDs) är "anonym" data och därför inte regleras i GDPR.

För många IAB medlemmar kan det vara lättast att behandla alla nätidentifierare som behandlas i utrustning, appar, verktyg och protokoll t ex ip-adresser, cookies eller andra identifierare som personlig data. Detta för att vara säker på att ni förstår var data kommer ifrån och för att få en tydlig bild vem ni delar datan med. IAB rekommenderar att genomföra en personuppgiftsrevision för att underlätta en sån här övning och kunna bevaka andra pågående datainsamlingsprocesser.

Från EU LEX: Fysiska personer kan knytas till nätidentifierare som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor, som radiofrekvensetiketter. Detta kan efterlämna spår som särskilt i kombination med unika identifierare och andra uppgifter som tas emot av servrarna, kan användas för att skapa profiler för fysiska personer och identifiera dem.

Laglig grund för behandling av personliga uppgifter

Organisationer måste ha en laglig grund för att lagligen hantera personuppgifter, inklusive insamlingen av data i första taget. GDPR anger sex lagliga grunder:

- Samtycke
- Kontrakt
- Rättsligt godkännande (med en annan lag)
- Skydda en persons vitala intressen
- Allmänintresse
- Intresseavvägning

De två rättsliga grunderna som används mest inom digital annonsering är **samtycke** och **intresseavvägning.** Tänk därför på de olika sätt som du behandlar data och identifiera vilken laglig grund som bäst passar hur du hanterar uppgifter. I en del fall kanske du anser det vara en blandning mellan samtycke och intresseavvägning, beroende på vilken slags bearbetning du tänkt göra och huruvida du hade tänkt använda uppgifterna för ytterligare ett syfte.
Det är viktigt att komma ihåg att under den nuvarande ePrivacydirektivet (”Cookie-lagstiftningen”) måste du inhämta samtycke för att få tillgång till och/eller lagra information på en användares enhet.

Europeiska Unionen går för tillfället igenom ePrivacy-direktivet vilket kan leda till stora förändringar för de kraven. Besök gärna IAB Europas sida om integritet och dataskydd. https://www.iabeurope.eu/category/policy/data-protection/

Samtycke

Samtycke har en framstående roll i GDPR. Men “samtycke” är bara en av sex rättsliga grunder som finns tillgängliga för företag som vill hantera uppgifter enligt specificerat ovan och det är i en del fall inte det mest passande. GDPR stramar upp villkoren för samtycke jämfört med de nuvarande reglerna: Generellt måste samtycket ges frivilligt, vara specifikt, informerat, tydligt och kräva en handling av individen för att vara giltig. Om du samlar personliga uppgifter måste samtycket vara uttalat.

Viktigast av allt, bevisbördan för att samtycke har givits på korrekt sätt ligger hos företaget. Att kunna bekräfta samtycke i de fall där man använder det som laglig grund är därför extremt viktigt, speciellt i de fall någon annan verksamhet samlar in samtycket åt dig.

ICO har nyligen publicerat utkast till riktlinjer för samtycket som snart kommer vara klara. Här hittar du rapporten. https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

Pseudonymisering

GDPR introducerar konceptet ”pseudonymisering” för första gången i EU dataskyddsförordningen. Vi tolkar det som att pseudonymisering inkluderar två

relaterade koncept. Pseudonymisering kan vara en process data genomgår- till exempel en kryptering, hashing eller tokenisering- för att försäkra att uppgifterna inte längre är direkt länkade till en individ. Personliga uppgifter som inte har några direkt identifierbara detaljer kan också bli pseudonymiserad vid tillfället det samlas in. Till exempel ett slumpmässigt ID som låter en användare bli igenkänd men inte direkt identifierad.
Oavsett måste företag komma ihåg att vilken form av pseudonymisering du än använder så förblir datan personlig under GDPR. Därmed sagt, det finns uppenbara fördelar med pseudonymisering som en utökad integritets- och säkerhetsåtgärd, inte minst då företag som pseudonymiserar uppgifter undgår vissa av GDPR's skyldigheter (läs mer under Individens rättigheter). Pseudonymisering kan också hjälpa i det balanseringstest du måste genomgå om du vill luta dig mot "allmänintresse" som stöd för din databehandling (se ovan).

Ta nu en titt på de meddelanden du redan använder, analysera vad som behöver ändras och inled förändringsarbetet om du inte redan har gjort det. Det är nödvändigt att alla organisationer som är involverade i att samla in och behandla data uppger den här information, från publicister hela vägen till relevanta tredje parter.

ICO Guidelines om privacy noticer, transparens och kontroll är ett bra ställe att börja. Titta även på "The right to be informed" kapitlet i ICO GDPR översikt. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Kommunicera information om integritetspolicy

Transparens är ett annat kärnämne inom GDPR. Integritetspolicys och notifieringar har länge använts inom digital marknadsföring för att kommunicera hur och varför organisationer använder uppgifter. GDPR kräver olika nivåer av detaljrikedom beroende på om du får uppgifterna direkt från individen eller inte. I samtliga fall måste ditt meddelande bland annat vara tydligt, lätt att hitta och skrivet i enkelt och tydligt språk. Det måste också inkludera den lagliga grund du använder som orsak till insamling och beskriva din intresseavvägning för att hantera personuppgifter om det är en av de grunder du använder.

Gå igenom dina processer för att försäkra dig om att du kan bemöta eventuella frågor du får från individer. Kom ihåg att om du pseudonymiserar uppgifter är du undantagen individens rättighet till tillgång, rättelse, radering, begränsning och dataportabilitet, så länge som individen inte aktivt ger dig mer information som gör det möjligt att identifiera dem (och du förväntar dig en låg reponsfrekvens).

Mer finns också att läsa EUR Lex. http://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A32016R0679

Individens rättigheter

GDPR ger individen omfattande rättigheter. Dessa är:

- Rätten att bli informerad
- Rätten till åtkomst
- Rätten till korrigering
- Rätten att glömmas
- Rätten att begränsa behandling
- Rätten till dataportabilitet (se Article 29 Working Party Guidance för mer detaljer)
- Rätten att protestera (rätten att avstå)
- Rätten att inte bli utsatt för en automatiserad beslutsprocess, inkluderat profilering.

Personuppgiftsansvarig och Personuppgiftsbiträde

GDPR står fast vid idén iden om ” Personuppgiftsansvarig” och ” Personuppgiftsbiträde” som man hittar i den nuvarande dataskyddsförordningen för att skilja mellan de olika rollerna organisationer spelar i hanteringen av personlig data. En påminnelse om hur de definieras: **Personuppgiftsansvarig** är organisationer som bestämmer, antingen ensamma eller tillsammans med andra Personuppgiftsansvariga, vem och varför personlig data samlas in. **Personuppgiftsbiträden** agerar å Personuppgiftsansvariges vägnar. Det betyder att enbart den Personuppgiftsansvarige är ansvarig för att följa dataskyddslagar enligt dagens regler, inte Personuppgiftsbiträdet.

Notera att GDPR utökar lagstadgade skyldigheter till Personuppgiftsbiträde. Det innebär att Personuppgiftsbiträde kan utsättas för genomdrivande/framtvingande/upprätthållande åtgärder av Dataskyddsmyndigheten och potentiella böter (upp till 4% av årlig global omsättning) från maj 2018. Under GDPR är skyldigheterna för Personuppgiftsbiträde bland andra:

Dataöverenskommelser- Personuppgiftsbiträden måste ha ett skrivet kontrakt (eller annan laglig handling) med Personuppgiftsansvarig. Det här kommer specificera ämnet, perioden för hanteringen, typen och syftet med insamlingen, typ av personlig data och kategorier av data subjekt och Personuppgiftsansvarig skyldigheter och rättigheter.

Datasäkerhet- Personuppgiftsbiträde måste ta passande säkerhetsåtgärder och informera Personuppgiftsansvarig ”utan otillbörlig fördröjning” vid en överträdelse (se nedan).

Underleverantörer- en Personuppgiftsbiträde kan endast använda underleverantörer med skriftlig tillåtelse från Personuppgiftsansvarige. Leverantörer måste också ge Personuppgiftsansvarige tillfälle att protestera mot ändringar i användandet av underleverantörer.

Personuppgiftsansvariges instruktioner – Personuppgiftsbiträde kan bara behandla personlig data i enlighet med instruktionerna från Personuppgiftsansvarig.

Ansvarsskyldighet- Personuppgiftsbiträde måste upprätta register av datahanteringsaktiviteter och göra dessa tillgängliga till relevant Dataskyddsmyndighet vid förfrågan.

Dataskyddsmyndighet – Personuppgiftsbiträde måste under vissa omständigheter utse ett Dataskyddsombud, se mer nedan.

Gränsöverskridande överföringar– Personuppgiftsbiträde måste följa restriktioner rörande gränsöverskridande överföringar, se mer nedan.

Eftersom både Personuppgiftsansvarige och Personuppgiftsbiträde kommer ha skyldigheter under GDPR är det viktigt för företag att tydliggöra sina roller. Till och med under en varumärkeskampanj kan rollerna ändras. Även om de är skrivna för nuvarande regler rekommenderar vi att du läser ICO’s guide i frågan för att få hjälp med till exempel hur du definierar din roll i målgruppssegmentering. Gör du det på egen hand eller endast efter instruktion från varumärken eller publicister. Skiljer det här sig mellan olika klienter? I vilket fall, börja med att skapa kontrakt med dina partners nu och se över de som redan finns för att se till de följer GDPR’s krav.

Dataöverträdelser

Överträdelser rörande personuppgifter kan få allvarliga konsekvenser, både i anseende- och finansiella termer. Du bör därför se till att du sätter in processer som låter dig upptäcka, rapportera och undersöka en överträdelse. Jämfört med existerande regler kräver GDPR att Personuppgiftsansvarige som har haft en överträdelse där individen riskerar att komma till skada, tex genom identitetsstöld eller genom en sekretessöverträdelse, kontaktar sin Dataskyddsmyndighet. Personuppgiftsbiträdet måste utan fördröjning meddela Personuppgiftsansvarig överträdelser som har skett av (se mer om Personuppgiftsansvarig och Personuppgiftsbiträde ovan).

Börja med att identifiera de typer av data som kan trigga meddelandebehovet. Informationsauditen nämnd tidigare kan hjälpa dig med det.

Kryptering och Integritetsanalys

Integritetsanalys Privacy Impact Assessments (PIAs)– eller Data Protection Impact Assessments (DPIAs) som GDPR kallar dem- spelar en viktig roll i de nya reglerna. Länge ansedd som god sed, blir det nu ett krav att göra en PIA i högrisksituationer, till exempel när ny teknologi testas eller där en profileringsmetod är sannolik att i stor utsträckning påverka individer. Det är än så länge oklart huruvida detta krav även kommer gälla behandlingen av pseudonym data.

Privacy by design (ditt företags icke-tekniska system för personuppgiftsskydd) och Privacy by default (de tekniska systemen) kodifieras med GDPR till lag. I båda fallen kan du genom en PIA utvärdera hur du ska inkludera de här två principerna i nya produkter eller tjänster som du vill lansera.

ICO har producerat riktlinjer rörande integritetsanalysen vilka utgör en bra startpunkt för genomgången. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Data Protection Officer (DPO)

GDPR stipulerar att ett av kriterierna för att bestämma om du behöver utse en Data Protection Officer (DPO)/ Dataskyddsombud (DSO) är där ”de huvudsakliga uppgifterna för Personuppgiftsansvarige eller Personuppgiftsbiträdets består av behandlingsprocesser som av sin natur, dess uppgift och/eller dess syfte kräver regelbunden och systematisk övervakning av data i stor skala”.

Om det här är relevant för ditt företag behöver du utse någon med ansvar för din GDPR-anpassning. Du behöver tänka på var i företagsstrukturen den här personen passar in.

För att få hjälp med detta läs Article 29 Working Party’s guidance on DPOs.

Internationellt

De flesta företag i vår bransch är verksamma över hela Europa. Om det här stämmer med ditt företag så måste du identifiera vilken Dataskyddsmyndighet som blir din ”centrala myndighet”.
Article 29 Working Party’s guidance on Lead Supervisory Authority kan hjälpa dig att bestämma vilken som blir din centrala myndighet.
Det återstår att se om UK också kommer bli ansedd tt hålla ”tillräcklig god standard” när det gäller datasäkerhet efter Brexit eller om en annan lösning kommer tas fram.

Du bör också fundera på dina val inför överföring av data till länder utanför EU. Du måste kanske göra det här för första gången om du inte tidigare har hanterat personlig data. GDPR erbjuder ett antal möjligheter för att föra data över landsgränser. Att föra över till länder som Europeiska kommissionen anser erbjuder en tillräcklig god säkerhetsstandard går utan hinder.

En lista på länder som har den här statusen hittar du här och den inkluderar EU- US Privacy Shield. Andra alternativ finns, inklusive standardiserade kontraktsklausuler.
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Du hittar checklistan och mer information på IAB Sveriges site

iabsverige.se/gdpr