Cybersikkerhet del II:

Sikring av at person-opplysninger forblir personlige

Når vi gir fra oss personopplysninger, for eksempel i forbindelse med netthandel, kan vi ikke være sikre på at virksomhetene håndterer disse personopplysningene på en forsvarlig måte. En ny EU-forordning skal bidra til dette.

Ph.D.
Arne Helme
Partner og leder for Cybersikkerhet i KPMG

Bruken av personopplysninger er i dag omfattende i alle sektorer. For oss som forbrukere ser vi det spesielt i nettbutikker. Ved hjelp av personopplysninger analyserer de vår oppførsel på nettet og enkelte nettbutikker gir forskjellige priser til ulike kunder. Ved hjelp av personopplysninger tilpasser nettbutikkene egne tjenester og produkter etter «vårt ønske», noe som kan oppleves som enkelt og bekvemmelig for oss.

Dette gjør også at håndtering, lagring og ikke minst sikringen av disse personopplysningene blir stadig mer kompleks. Hvordan skal virksomheter håndtere disse personopplysningene på en forskriftsmessig måte og tilfredsstille de lovpålagte kravene til personvern? Hvordan skal vi som forbrukere vite at virksomhetene imøtekommer kravene?

Manglende sikring av personopplysningene i norske nettbutikker

En ny undersøkelse gjennomført av KPMG viser at forbrukere bør være seg langt mer bevisste på hvilke personopplysninger de oppgir når de handler på nett. I undersøkelsen har KPMGs cybersikkerhetsteam opprettet kundekontoer (uten å gjennomføre en handel) på 40 av landets ledende nettbutikker, og de har vurdert hva som kreves av personopplysninger.

Navn, adresse og postnummer ber de fleste nettstedene om, noe som er naturlig i en nettbutikk. I tillegg kreves det flere steder kjønn, telefonnummer, fødselsdag og personnummer.

Det er ingen grunn til at nettbutikker trenger personnummeret ditt for å opprette en konto. Dette er en opplysning vi aldri ville ha oppgitt om vi hadde gått inn i en fysisk butikk. På nettet tar vi gjerne litt lettere på slike ting, men vi må ikke glemme at vi selv er ansvarlige for opplysningene vi gir fra oss.

For vet vi egentlig hvordan disse opplysningen blir lagret og håndtert? I undersøkelsen forsøkte Cyber-teamet også å avslutte kontoene. På 16 av 40 sider ble kontoen stengt innen én dag (noe som ikke automatisk betyr at personopplysningene blir slettet). På kun to steder kunne man gjøre dette selv på nett, på de resterende måtte man ta kontakt med kundeservice, enten via epost, chat eller telefon. På fire nettbutikker måtte de ta en telefonsamtale for å gjøre dette. Fem steder sa at de ville sperre kontoen, mens ni nettbutikker ikke svarte.

Noen nettbutikker opplyste at de stengte kontoen, men at de fortsatt ville lagre opplysningene. Med andre ord, opplysningen forblir i systemet uten at man vet hvordan de vil bli brukt i fremtiden. Dette er ikke i henhold til riktig håndtering av personopplysninger.

Global usikkerhet knyttet til personvern

Dette aspektet gjenspeiles også i en ny undersøkelse fra KPMG globalt, «Crossing the line», der 6900 respondenter i 24 land har deltatt.

Færre enn ti prosent føler ifølge undersøkelsen at de har kontroll på hvordan nettsteder håndterer våre personopplysninger. 55 prosent sier også at de har avsluttet en netthandel grunnet bekymring for om personvernet blir ivaretatt. En av undersøkelsens konklusjoner er at virksomheter i dag svikter når det gjelder å se personvern som en grunnleggende prioritet, og at det ofte er risiko for at de skal «gå over streken». Virksomheter må ikke glemme at forbrukere flest er mer opptatt av personvern enn økt bekvemmelighet.

Ny EU-forordning skal styrke personvernet

Å sikre et godt personvern er gjenstand for diskusjon også i EUs indre gemakker. I mai 2018 trer en ny personvernforordning i kraft (eng.: *The General Data Protection Regulation* – GDPR). Dette er EUs krav til behandling av personopplysninger utført av virksomheter som er etablert i EU. Etter hele fire år med forhandlinger mellom europeiske lovgivere er forordningen et sterkt og globalt signal om at Europa fortsatt tar personvern på største alvor.

Personvernforordningen er utvilsomt et sterkt lovverk som representerer et vesentlig skifte sammenlignet med nåværende personvernlovgivning innen EU. For første gang vil vi få et sett med personvernregler som gjelder på tvers av alle land i EU, noe som innebærer en harmonisering av regelverket i EU. Denne harmoniseringen går også enda lenger, siden personvernforordningen i visse tilfeller også gjelder for virksomheter etablert utenfor EU, for eksempel for virksomheter som tilbyr varer og tjenester til personer i EU.

Hvilke konsekvenser får nytt regelverk?

For de fleste virksomhetene haster det med å få kartlagt hvor mye arbeid de må gjøre for å etterleve dette nye regelverket. Blant endringene er at det ikke lenger vil være akseptabelt å operere med generelle samtykker. Virksomheten må tilby brukere et mer nyansert valg, hvor de må gis mulighet til å godkjenne én form for databruk, men kunne avslå en annen. Det vil være pålagt rapportering av avviksmelding (fortrinnsvis innen 72 timer). Det vil si at sikkerhetsbrudd som medfører ulovlig behandling av personopplysninger, skal meldes til tilsynsmyndigheter, uavhengig av størrelse og utfall. Dette medfører også økte krav til loggføring og dokumentering av sikkerhetsbrudd. Forbrukere skal ha retten til å bli glemt. Med andre ord, hver enkelt av oss skal ha rett til å kreve at personopplysninger blir slettet. Dette krever at virksomhetene har svært god oversikt over hvor personopplysninger er lagret og hvordan de behandles. Det blir også påbudt med personvernombud for en rekke virksomheter. Påbudet gjelder blant annet for virksomheter med håndtering av data som sin kjernevirksomhet og for de som innehar større mengder sensitive data.

Det nye regelverket vil på sikt styrke forbrukernes eierskap til egne opplysninger og stille de nødvendige kravene til virksomheter. La det ikke være tvil, vi er fremdeles selv ansvarlige for opplysningene vi gir fra oss på nettet, men samtidig skal vi ha visshet om at de blir håndtert og lagret på en forskriftmessig god måte.

Riktig behandling av nettolønn

11. mai 2016 ble en merkedag for alle som jobber med nettolønn. Høyesterett satte med Biller-dommen et endelig punktum for en diskusjon som har pågått i årevis mellom Skatteetaten, rådgivere, personlige skattytere, interesseorganisasjoner og selskaper med ansatte som jobber på tvers av landegrensene.

Advokat
Cathrine Bjerke Dalheim
Partner KPMG Law Advokatfirma

Advokat/Partner KPMG Law Advokatfirma
Gjertrud H. Behringer
KPMG Law Advokatfirma

I korte trekk var skatteetatens klare oppfatning at oppgrossing av nettolønn skulle gjøres med norske skattesatser og at faktisk betalt skatt i utlandet var irrelevant. Skatteetatens syn var at det skulle beregnes en fiktiv lønn og at den reelle, mottatte fordelen ikke var relevant ved fastsettelse av bruttolønn. I Biller-dommen ble det imidlertid lagt til grunn at en personlig skattyter bare skal skattlegges for den *fordelen* vedkommende faktisk mottar. Hovedbegrunnelsen til flertallet var henvisningen til skattelovens fordelsbegrep og at «fordelen er det skattyter mottar som dekning i form av lønn og arbeidsgivers dekning av skatt og eventuell trygdeavgift». Arbeidsgivers dekning av skatt skal med andre ord likestilles med en hvilken som helst annen naturalytelse som eksempelvis telefon, avis, dekning av bolig, bil etc.

Tabellen under illustrer rettstilstanden før og etter Biller-dommen:

	Oppgrosset bruttolønn før dommen	**Oppgrosset bruttolønn etter dommen**
Nettolønn	1 000 000	
Norske satser	1 661 943	
Skatt utland (kr 200 000) og norsk trygdeavgift		1 307 190