Extern informationssäkerhetspolicy

1. Bakgrund

Svenska Postkodlotteriet AB driver lotteri på uppdrag av Svenska Postkodföreningen, som innehar en spellicens utfärdad av Spelinspektionen (”Postkodlotteriet”). Postkodlotteriet arbetar ständigt för att säkerställa att kunderna ska känna sig trygga och ha förtroende för den verksamhet som bedrivs. En viktig del är att den information som hanteras i verksamheten hanteras på ett tryggt och korrekt sätt. Som stöd för detta har Postkodlotteriet antagit denna informationssäkerhetspolicy som gäller för hela verksamheten samt våra samarbetspartners.

2. Postkodlotteriets hantering

Postkodlotteriet arbetar med informationssäkerhet som en naturlig del av verksamheten och tar stöd av ISO27001 standarden för att uppnå adekvat säkerhetsnivå. Postkodlotteriets utgångspunkt är att ***information är en tillgång*** som är avgörande för verksamheten och som därför måste skyddas. Att inte skydda information eller inte hantera information på ett korrekt sätt kan leda till allvarliga skador på Postkodlotteriets varumärke, allvarliga skador för tredjeman, kritiska störningar i verksamheten samt lagbrott.

Postkodlotteriets åtagande gentemot kunder, medarbetare och andra intressenter är att arbeta på ett systematiskt och målmedvetet sätt för att skydda den information som hanteras i fråga om **konfidentialitet**, **riktighet** och **tillgänglighet**.

Information kan lagras i olika former; digitalt, fysiskt eller i form av den kunskap som finns hos medarbetarna. Information kan också överföras på olika sätt; fysiskt, elektroniskt eller muntligt. Oavsett i vilken form eller plats informationen behandlas eller på vilket sätt den överförs så ska den alltid skyddas på lämpligt sätt.

Postkodlotteriet gör detta genom att:

1. Identifiera, dokumentera, implementera och uppfylla gällande lagkrav, praxis, avtalsbaserade krav och krav enligt tillämpliga standarder
2. Identifiera, styra och skydda verksamhetens processer
3. Identifiera och klassificera information samt styra och kontrollera användares rättigheter och access till information
4. Säkerställa att information är tillgänglig och korrekt när den behövs
5. Identifiera, dokumentera och prioritera informationssäkerhetsrisker samt införa och dokumentera de åtgärder som behövs för att hantera dessa risker
6. Vidmakthålla en hög medvetenhet kring informationssäkerhet genom bl.a tydliga informationssäkerhetsmål, regelbundna utbildningar, uppdateringar kring hot och sårbarheter
7. Tillhandahålla en säker arbetsplats med arbetssätt och handlingsplaner för att upptäcka och hantera avvikelser
8. Identifiera och ställa relevanta krav på samarbetspartners som hanterar Postkodlotteriets information samt följa upp att kraven uppfylls
9. Mäta och följa upp vår prestanda i fråga om informationssäkerhet
10. Identifiera avvikelser och förbättringsmöjligheter, samt prioritera och genomföra kontinuerliga förbättringar av våra arbetssätt och processer

3. Krav på samarbetspartners

Postkodlotteriet ställer krav på att samarbetspartners lever upp till en adekvat säkerhetsnivå.

Det ska därför finnas åtgärder på plats för att skydda och säkerställa en korrekt hantering av den information som hanteras åt eller för Postkodlotteriet.

Postkodlotteriet ställer krav på att samarbetspartners tillser att alla som har tillgång till information som tillhandahållits av Postkodlotteriet är bundna av minst motsvarande sekretess som följer av mellan parterna föreliggande avtal och har anpassad behörighet som med regelbundna intervall kontrolleras och loggas. Sådan sekretess ska gälla även i kontakter med myndigheter.

Om en samarbetspartner använder underleverantörer kräver Postkodlotteriet att samarbetspartnern ansvarar för sina underleverantörer såsom för egen del, samt att samarbetspartnern tillser att underleverantören (i alla led) skyddar och hanterar information enligt avtal. Postkodlotteriet ska förhandsgodkänna om underleverantören ska lagra, behandla eller transportera informationen.

3.1. Avvikelsehantering

Om något oförutsett inträffar med Postkodlotteriets information då den hanteras aven samarbetspartners, tex att processer frångås eller information hamnar i orätta händer eller överförs oskyddad, ska det finnas möjlighet att enkelt upptäcka dessa avvikelser. Det ska finnas väl fungerande rutiner för upptäckt och hantering av informationssäkerhetsavvikelser. Exempelvis:

- Rutiner för att upptäcka sådana avvikelser
- Åtgärdsplan för begränsning av skada vid avvikelser
- Avvikelse-/incidentrapportering

Vid inträffande av avvikelser ska Postkodlotteriet kontaktas.

Dessutom ska det finnas tekniska och praktiska åtgärder för att möjliggöra utredning av möjliga och misstänkta avvikelser avseende information. Exempelvis:

- Obehörig åtkomst
- Förstörelse
- Förlust
- Förändring

3.2. Uppföljning

Postkodlotteriet kräver en rätt att själv eller med hjälp av tredje part, följa upp att samarbetspartners agerar i enlighet med avtal samt att samarbetspartners ska vara skyldig att ge sådant stöd som krävs för att utföra sådan kontroll.

3.3. Överföring

Det föreligger ett generellt förbud mot överföring av information till länder utanför EU/EES. Under vissa förutsättningar är det ändock tillåtet att överföra information utanför EU/EES. Det förutsätter att:

- det finns ett beslut från EU-kommissionen om att exempelvis ett visst land utanför EU/EES säkerställer så kallad adekvat skyddsnivå;
- leverantören har vidtagit lämpliga skyddsåtgärder, till exempel bindande företagsbestämmelser eller standardavtalsklausuler; eller
- särskilda situationer och enstaka fall såsom avses enligt GDPR föreligger.

3.4. Efter avslutat avtal

I samband med avslut av avtal kräver Postkodlotteriet att samarbetspartners säkerställa att följande sker:

- Radera, återlämna eller vidta annan åtgärd avseende informationen enligt Postkodlotteriets instruktion, samt
- Skriftligen intyga att relevant åtgärd har vidtagits.