PSA
LEGAL COUNSELLORS

# डिजिटल व्यक्तिगत डेटा सुरक्षा अधिनियम, 2023 और मसौदा नियम, 2025

## व्यवसायों के लिए अंतर्दृष्टि

इस पुस्तक का अंग्रेजी से हिंदी में अनुवाद AI का उपयोग करके किया गया है, इसमें कुछ त्रुटियाँ हो सकती हैं।

PSA LEGAL COUNSELLORS

# अंतर्वस्तु


1 संक्षिप्त शब्द.....2

2 डीपीडीपी नियम - एक सचित्र में प्रमुख विशेषताएँ.....3

3 अवधारणा 1: डीपीडीपीए और मसौदा नियमों के अंतर्गत सहमति और सूचना की आवश्यकताएँ.....7

4 अवधारणा 2: सहमति प्रबंधक.....9

5 क्या होगा यदि “सहमति” पर ये जीडीपीआर मामले भारत में घटित होते?.....12

6 अवधारणा 3: महत्वपूर्ण डेटा फिड्युसरी.....17

7 अवधारणा 4: फिड्युशियरी-प्रोसेसर संबंध का प्रबंधन करना.....19

8 अवधारणा 5: आयु सीमा.....22

9 अवधारणा 6: डेटा संरक्षण .....24

10 अवधारणा 7: यूरोपीय संघ से भारत तक: डेटा विषय/प्रमुख अधिकारों की समझ.....30

11 क्या होगा यदि "डेटा विषय अधिकार" पर ये जीडीपीआर मामले भारत में घटित हों?.....34

12 अवधारणा 8: डेटा उल्लंघन.....39

13 क्या होगा यदि "व्यक्तिगत डेटा उल्लंघन" पर ये जीडीपीआर मामले भारत में घटित हों?.....42

13 अवधारणा 9: साइबर बीमा.....49

## परिवर्णक शब्द

**CERT-In:** भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम
**सीजी:** केंद्र सरकार
**डीसी:** डेटा नियंत्रक
**डीएफ:** डेटा फ़िड्युसरी
**डीपी:** डेटा प्रिंसिपल
**डीपीए:** डेटा प्रोसेसिंग समझौता
**डीपीबीआई:** डेटा प्रोटेक्शन बोर्ड ऑफ़ इंडिया
**डीपीडीपीए:** डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023
**डीपीआईए:** डेटा प्रोटेक्शन इम्पैक्ट असेसमेंट
**डीपीओ:** डेटा प्रोटेक्शन ऑफिसर
**डीपीआर:** डेटा प्रोसेसर
**डीपीडीपी नियम या विनियम:** ड्राफ्ट डिजिटल पर्सनल डेटा प्रोटेक्शन नियम, 2025
**डीएस:** डेटा विषय (जीडीपीआर के तहत एक पहचान योग्य प्राकृतिक व्यक्ति)
**जीडीपीआर:** सामान्य डेटा सुरक्षा विनियमन
**IT अधिनियम:** सूचना प्रौद्योगिकी अधिनियम, 2000
**MeitY:** इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय
**पीडी:** व्यक्तिगत डेटा
**PETs:** गोपनीयता संवर्धन उपकरण
**एसडीएफ:** महत्वपूर्ण डेटा फ़िड्युसरी
**SDPI नियम:** सूचना प्रौद्योगिकी (उचित सुरक्षा अभ्यास और प्रक्रियाएं और संवेदनशील व्यक्तिगत जानकारी) नियम, 2011

**नोट 1:** भारतीय रुपए को 85 रुपये प्रति अमेरिकी डॉलर की दर से अमेरिकी डॉलर में परिवर्तित किया गया है और पूर्णांकित किया गया है।

## डेटा प्रिंसिपल को सूचित करें

धारा 5 के अनुसार, डीएफ को किसी भी डेटा को संसाधित करने से पूर्व डीपी को सूचित करना अनिवार्य है।

अब, नियम 3 यह स्पष्ट करता है कि यह नोटिस स्वतंत्र, स्पष्ट और सरल भाषा में होना चाहिए, और इसमें पीडी, निर्दिष्ट उद्देश्य, तथा सक्षम किए जाने वाले सामान/सेवाओं या उपयोगों का विस्तृत विवरण शामिल होना चाहिए।

इसमें सहमति वापस लेने की प्रक्रिया (सहमति देने के समान सरलता से), डीएस अधिकार और डीपीबीआई को शिकायत प्रस्तुत करने की विधि भी शामिल होगी।

सहमति वापस लेने का विकल्प, निस्संदेह, सहमति के समान ही विस्तृत होना चाहिए।

## सहमति प्रबंधक

धारा 6(7) में सहमति प्रबंधक का प्रावधान है। नियम 4 के अनुसार, सहमति प्रबंधक को

- एक भारतीय संगठन होना चाहिए
- न्यूनतम निवल संपत्ति 20 मिलियन रुपये या लगभग 2,35,000 अमेरिकी डॉलर होनी चाहिए
- डीपी के प्रति प्रत्ययी क्षमता पर कार्य करना चाहिए
- उप-अनुबंध न करें और न ही अपने दायित्वों को सौंपें
- डीएफ के साथ किसी भी प्रकार के हितों के संघर्ष से बचें

प्रथम अनुसूची में विस्तृत जानकारी।

## कुछ परिस्थितियों में प्रक्रिया

धारा 7(बी) या 17(2)(बी) के अंतर्गत पीडी पर कार्रवाई करते समय राज्य या उसके उपक्रमों को दूसरी अनुसूची का पालन करना अनिवार्य होगा।

इसमें वैध प्रसंस्करण, डेटा न्यूनतमकरण, उद्देश्य सीमांकन और उचित सुरक्षा उपायों को सुनिश्चित करना शामिल है।

इस प्रकार, राज्य ने डीएफ के रूप में कार्य करते समय अपने ऊपर अत्यधिक कठोर दायित्व ले लिया है।

## डेटा उल्लंघन की सूचना

धारा 8(6) के अनुसार, डीएफ को प्रत्येक प्रभावित डीपी और डीपीबीआई को पीडी उल्लंघनों के संबंध में सूचित करना अनिवार्य है।

नियम 7 स्पष्ट करता है कि डेटा उल्लंघनों की रिपोर्ट "बिना देरी" के (ए) प्रत्येक प्रभावित डीपी को उल्लंघन, प्रासंगिक परिणामों, शमन कदमों और सुरक्षा उपायों के विवरण के साथ, और (बी) डेटा प्रोटेक्शन ब्यूरो को उल्लंघन और उसके संभावित प्रभाव के विवरण के साथ की जानी चाहिए। इसके अतिरिक्त, 72 घंटों के भीतर, उल्लंघन, शमन कदमों, जिम्मेदार व्यक्ति के विवरण, उपचारात्मक उपायों और डीपी को अधिसूचनाओं की रिपोर्ट के विवरण के साथ डेटा प्रोटेक्शन ब्यूरो को एक अद्यतन रिपोर्ट प्रदान की जानी चाहिए। यह सभी उल्लंघनों पर लागू होगा, चाहे नुकसान कितना भी हो।

संभवतः, यह आवश्यकता डीपी को अभिभूत कर देगी और डीएफ तथा डीपीबीआई पर बोझ बढ़ा देगी। इसलिए, डीएफ को अपनी डेटा सुरक्षा टीमों को सुदृढ़ करना चाहिए। हमें आशा है कि सेकऑप्स की नियुक्तियों में उल्लेखनीय वृद्धि होगी और डेटा ब्रीच/साइबर सुरक्षा बीमा प्रस्तावों में वृद्धि होगी।

## उचित सुरक्षा प्रावधान

धारा 8(5) के अनुसार, डीएफ को पीडी उल्लंघनों को रोकने के लिए उपयुक्त सुरक्षा उपाय करने की आवश्यकता है।

हालांकि कोई विशेष सुरक्षा उपाय निर्धारित नहीं किए गए हैं, नियम 6 में कुछ न्यूनतम मानक निर्धारित किए गए हैं, जैसे एन्क्रिप्शन/मास्किंग/वर्चुअल टोकन के माध्यम से पीडी की सुरक्षा, उचित एक्सेस कंट्रोल का कार्यान्वयन, अनधिकृत एक्सेस का पता लगाने के लिए लॉग बनाए रखना, डेटा बैकअप आदि। इससे छोटे डीएफ पर बोझ पड़ सकता है। यह कहा जा रहा है कि इन सभी सुरक्षा उपायों को उस तरीके से लागू किया जा सकता है जिसे डीएफ उचित समझे।

इसके अतिरिक्त, डीएफ को डेटा उल्लंघन लॉग को एक वर्ष तक या किसी अन्य कानून द्वारा विशेष रूप से निर्धारित अवधि तक संरक्षित करना होगा।

## पूछताछ हेतु संपर्क विवरण

धारा 6(3) के अनुसार, डीएफ को डीपीओ (जहां लागू हो) या डीपी की पूछताछ का उत्तर देने के लिए अधिकृत किसी अन्य व्यक्ति का व्यावसायिक संपर्क विवरण प्रदान करना अनिवार्य है।

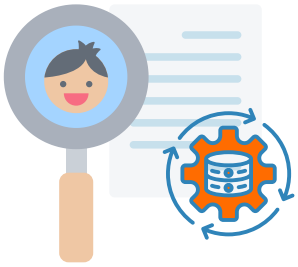
नियम 9 स्पष्ट करता है कि यह संपर्क जानकारी डीएफ की वेबसाइट/ऐप पर प्रदर्शित की जानी चाहिए और डीपी के साथ सभी संचार में शामिल की जानी चाहिए। यह स्पष्ट नहीं है कि ऐसा अधिकृत व्यक्ति, जो डीपीओ नहीं है, पर कोई दायित्व होगा या नहीं।

## डेटा संरक्षण और डेटा नष्ट करना

डीएफ को पीडी को हटाना आवश्यक है जब वे उचित रूप से यह मान लेते हैं कि डेटा अब अपने उद्देश्य की पूर्ति नहीं कर रहा है (धारा 8(7)) और जब कोई डीपी अपनी सहमति वापस ले लेता है (धारा 12(3))।

इन आवश्यकताओं का एकमात्र अपवाद तब है जब डेटा को किसी कानून के तहत बनाए रखने की आवश्यकता हो। नियम 8 केवल तीन प्रकार के डीएफ के लिए पीडी को हटाने और बनाए रखने का प्रावधान करता है, अर्थात् (ए) भारत में 20 मिलियन या अधिक पंजीकृत उपयोगकर्ताओं वाली ई-कॉमर्स संस्थाएं; (बी) भारत में 20 मिलियन या अधिक पंजीकृत उपयोगकर्ताओं के साथ सोशल मीडिया मध्यस्थ; और (सी) भारत में 5 मिलियन या अधिक पंजीकृत उपयोगकर्ताओं के साथ ऑनलाइन गेमिंग मध्यस्थ। ऐसी संस्थाएं अंतिम इंटरैक्शन या नियमों के प्रारंभ से 3 वर्षों तक पीडी को बनाए रख सकती हैं। इन डीएफ को अपने पीडी को हटाने से 48 घंटे पहले डीपी को सूचित करना आवश्यक है। किसी अन्य प्रकार के डीएफ के लिए कोई समयसीमा का उल्लेख नहीं किया गया है।

## बच्चे के व्यक्तिगत डेटा का संसाधन



धारा 9(1) के अंतर्गत, किसी बच्चे या संरक्षकता के तहत किसी व्यक्ति के डेटा को संसाधित करने से पूर्व, डीएफ को माता-पिता या अभिभावक से सत्यापन योग्य सहमति प्राप्त करनी आवश्यक है। नियम 10 के अनुसार, डीएफ को यह सुनिश्चित करना होगा कि "माता-पिता" एक पहचान योग्य वयस्क हैं। यह स्पष्ट नहीं है कि डीएफ को उन मामलों का कैसे समाधान करना चाहिए जहां कोई बच्चा झूठा दावा करता है कि वह वयस्क है। नियम 10 डीपी की आईडी और आयु से संबंधित वर्चुअल टोकन का भी उल्लेख करता है। यदि इसे अपनाया जाता है, तो भारत ऐसी उन्नत आयु-निर्धारण तकनीक को लागू करने वाले पहले देशों में से एक बन सकता है।

नियम 11 के अंतर्गत, स्वास्थ्य सेवा प्रदाता, शैक्षणिक संस्थान, चाइल्डकेयर प्रदाता आदि जैसी कुछ संस्थाओं को धारा 9(1) और 9(3) (बच्चों की ट्रैकिंग, व्यवहार की निगरानी या लक्षित विज्ञापन पर रोक) के अनुपालन से छूट दी गई है। जबकि धारा 9(1) की छूट उचित प्रतीत होती है, धारा 9(3) की छूट इन संस्थाओं को बच्चों को लक्षित विज्ञापन देने की अनुचित अनुमति प्रदान कर सकती है।

चौथी अनुसूची डीएफ को धारा 9 (1) और (3) के अनुपालन से छूट प्रदान करती है, जहां प्रसंस्करण के उद्देश्यों में कानूनी कर्तव्य, बच्चे के लाभ आदि शामिल हैं। हालाँकि, ये अभिव्यक्तियाँ अस्पष्ट हैं, और यह स्पष्ट नहीं है कि इनकी व्याख्या किस प्रकार की जाएगी।

## एसडीएफ का अतिरिक्त उत्तरदायित्व

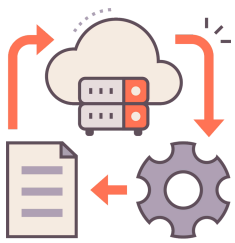
धारा 10(2) राज्य को किसी भी डीएफ को एसडीएफ के रूप में अधिसूचित करने का अधिकार प्रदान करती है। नियम यह निर्धारित करने के लिए कोई मानदंड नहीं प्रस्तुत करते कि कौन एसडीएफ के रूप में योग्य है। धारा 35, नियम 22(1) के साथ मिलकर, केंद्र सरकार को किसी भी डीएफ से डेटा प्राप्त करने की अनुमति देती है ताकि यह निर्धारित किया जा सके कि इसे महत्वपूर्ण के रूप में वर्गीकृत किया जाना चाहिए या नहीं।

नियम 12 के तहत, एसडीएफ को वार्षिक डीपीआईए और ऑडिट करना अनिवार्य है और डीपीबीआई को अपनी टिप्पणियों की रिपोर्ट प्रस्तुत करनी चाहिए। एसडीएफडी को यह सुनिश्चित करना चाहिए कि पीडी को संसाधित करने के लिए उपयोग किया जाने वाला कोई भी "एल्गोरिदमिक सॉफ़्टवेयर" डीपी के अधिकारों के लिए कोई जोखिम उत्पन्न न करे। यह स्पष्ट नहीं है कि सम्यक् तत्परता कैसे किया जाना चाहिए। केंद्र सरकार भारत में कुछ पीडी (इसके प्रवाह से संबंधित ट्रैफ़िक डेटा सहित) को संसाधित करने के लिए एसडीएफ की आवश्यकता हो सकती है। यह डेटा स्थानीयकरण को लागू करने का एक अप्रत्यक्ष तरीका प्रतीत होता है और यदि किसी विशिष्ट डेटा सेट को सीमा पार हस्तांतरण से प्रतिबंधित किया जाता है, तो अनुपालन की लागत में काफी वृद्धि हो सकती है।

## डेटा प्रिंसिपल के अधिकारों

अध्याय III (धारा 11 से 15) डीपी अधिकार प्रदान करता है, जैसे कि सूचना तक पहुँच, व्यक्तिगत जानकारी में सुधार और उसे मिटाना, सहमति वापस लेना और नामांकन। नियम 13 में डीएफ और सहमति प्रबंधक को अपनी वेबसाइट/ऐप पर डीपी के लिए इन अधिकारों तक पहुँचने की विधि प्रकाशित करने की आवश्यकता है। आगे बढ़ते हुए, हम आशा करते हैं कि डीएफ इन अधिकारों को सुविधाजनक बनाने के लिए सॉफ़्टवेयर समाधान लागू करेंगे।


## भारत के बाहर पी.डी. प्रसंस्करण



धारा 16 सीजी अन्य देशों में व्यक्तिगत डेटा हस्तांतरण पर प्रतिबंध लगाने का अधिकार प्रदान करती है। नियम 14 के अनुसार, डीएफ को भारत से सम्बंधित डीपी के डेटा प्रोसेसिंग करने वाले किसी भी विदेशी देश या विदेशी संस्था को व्यक्तिगत डेटा उपलब्ध कराने के संबंध में सीजी के निर्देशों का पालन करना अनिवार्य है। इससे भारत के बाहर डेटा प्रोसेसिंग करने वाले डीएफ के लिए अनुपालन संबंधी चुनौतियाँ उत्पन्न हो सकती हैं, क्योंकि उन्हें विदेशी कानूनों का भी पालन करना पड़ सकता है।

## भारतीय डेटा सुरक्षा बोर्ड

धारा 18 में डीपीबीआई की स्थापना का प्रावधान है। नियम इस पर विस्तार से चर्चा करते हैं और सदस्यों की नियुक्तियों, सेवा की शर्तों तथा अन्य प्रक्रियाओं के बारे में विस्तृत जानकारी प्रदान करते हैं। नियम 19 में स्पष्ट किया गया है कि डीपीबीआई एक डिजिटल कार्यालय के रूप में कार्य करेगा, जिसमें भौतिक उपस्थिति की आवश्यकता के बिना कार्यवाही करने के लिए तकनीकी-कानूनी उपायों का उपयोग किया जाएगा। नियमों की चौथी और पाँचवीं अनुसूची डीपीबीआई और उसके कर्मचारियों की सेवा की शर्तों को कवर करती है।

# अवधारणा 1: डीपीडीपीए और मसौदा नियमों के अंतर्गत सहमति और सूचना की आवश्यकताएँ

## 1. कानून क्या दर्शाता है?

डीपीडीपीए व्यक्तिगत डेटा की प्रोसेसिंग के लिए दो कानूनी आधार प्रदान करता है: (ए) सहमति, और (बी) कुछ वैध उपयोग (धारा 4 (1))। जब सहमति व्यक्तिगत डेटा की प्रोसेसिंग का आधार होती है, तो यह निम्नलिखित मानदंडों को पूरा करना चाहिए: (ए) स्वतंत्र, (बी) विशिष्ट, (सी) सूचित, (डी) बिना शर्त, और (ई) स्पष्ट, जिसमें एक स्पष्ट सकारात्मक कार्रवाई शामिल है जो दर्शाती है कि डीपी निर्दिष्ट उद्देश्य के लिए अपने व्यक्तिगत डेटा की प्रोसेसिंग के लिए सहमत है, और उस उद्देश्य को पूरा करने के लिए आवश्यक व्यक्तिगत डेटा तक सीमित है (धारा 6 (1))।

**सहमति के लिए अनुरोध**

सहमति के लिए प्रत्येक अनुरोध को स्पष्ट और सरल भाषा (अंग्रेजी या आठवीं अनुसूची की अन्य भाषाएँ) में प्रस्तुत किया जाना चाहिए, और इसमें डीपीओ (जहाँ लागू हो) या डीपी से संचार के लिए नामित किसी अन्य व्यक्ति का विवरण शामिल होना चाहिए। सहमति के लिए अनुरोध के साथ या पहले एक स्वतंत्र "सूचना" होना आवश्यक है।

## 2. डीपी को भेजे जाने वाले नोटिस में क्या समाहित होना चाहिए?

डीपी को नोटिस स्पष्ट और सरल भाषा में (अंग्रेजी या आठवीं अनुसूची की किसी अन्य भाषा) प्रदान किया जाना चाहिए, जिसमें डीपी को सूचित सहमति देने के लिए आवश्यक वि वरण शामिल होना चाहिए, जिसमें न्यूनतम शामिल है।

- प्राप्त किए जाने वाले पीडी का मदानुसार विवरण
- उद्देश्य जिसके लिए पीडी संसाधित किया जाना है, साथ ही वस्तुओं और सेवाओं का विस्तृत विवरण
- डेटा फिड्युसरी की वेबसाइट/ऐप तक पहुंचने के लिए संचार लिंक, साथ ही डेटा प्रिंसिपल के माध्यम से अन्य कोई साधन:
  - अपनी सहमति वापस लें
  - अपने अधिकारों का उपयोग करें (शिकायत निवारण के अधिकार सहित)
  - डीपीबीआई में शिकायत दर्ज कराएँ

(धारा 5(1) और (3) ड्राफ्ट नियम 3 के अंतर्गत)

**विरासत डेटा के लिए सहमति**

जहाँ डीपी ने डीपीडीपीए के आरंभ होने से पूर्व सहमति दी है, वहाँ डीएफ को शीघ्रता से, उपरोक्त विवरणों (धारा 5(2)(ए)) के साथ एक नोटिस जारी करना चाहिए। परिणामस्वरूप, हमारा सुझाव है कि डीएफ को डीपीडीपीए के आरंभ से पूर्व एकत्रित सभी विरासत पीडी की पहचान करनी चाहिए और इसे इसके संग्रह के उद्देश्य से मानचित्रित करना चाहिए। आवश्यक नोटिस जारी करने के पश्चात, डीएफ तब तक प्रसंस्करण जारी रख सकते हैं जब तक कि डीपी द्वारा सहमति वापस नहीं ली जाती (धारा 5(2)(बी))।

## 3. प्रमुख प्रश्न

### (क) क्या सहमति को वापस लिया जा सकता है?

जहां डीपी ने पीडी की प्रक्रिया के लिए सहमति दी है, वह किसी भी समय अपनी सहमति वापस ले सकती है। वापसी की प्रक्रिया सहमति देने की प्रक्रिया के समान सरल होनी चाहिए (धारा 6(4))। सहमति की इस वापसी से पूर्व की प्रक्रिया की वैधानिकता पर कोई प्रभाव नहीं पड़ेगा (धारा 6(5))।

### (ख) सहमति वापस लेने के पश्चात डीएफ को क्या करना चाहिए?

डीपी द्वारा पीडी के प्रसंस्करण के लिए अपनी सहमति वापस लेने के पश्चात, डीएफ को आवश्यक है

- उचित समय के भीतर, अपने डीपीआर को पीडी की प्रोसेसिंग को रोकने के लिए बाध्य करें/सुनिश्चित करें, जब तक कि डीपीडीपीए, ड्राफ्ट नियमों या किसी अन्य लागू कानून (धारा 6(6)) के तहत प्रोसेसिंग की आवश्यकता न हो या उसे अधिकृत न किया गया हो।
- डीपी की पीडी को समाप्त कर दें, जब तक कि लागू कानून के अनुपालन के लिए इसे बनाए रखना आवश्यक न हो (धारा 8(7)(ए))।

### (ग) सहमति प्रबंधक कौन हैं?

एक डीपी "सहमति प्रबंधक" के माध्यम से अपनी सहमति प्रदान कर सकता है, प्रबंधित कर सकता है, समीक्षा कर सकता है या वापस ले सकता है। ऐसे नियुक्त सहमति प्रबंधक को डीपीबीआई के साथ पंजीकृत होना आवश्यक है और डीपी के प्रति उत्तरदायी रहना चाहिए (धारा 6(7) से 6(9))।

**आगे बढ़ने का मार्ग**

डीपीडीपीए वैध सहमति प्राप्त करने में विफल रहने पर 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाता है। अनुपालन सुनिश्चित करने के लिए, कंपनियों को सूचीबद्ध आवश्यकताओं के अनुसार अपनी सहमति तंत्र और गोपनीयता नोटिस को अद्यतन करना आवश्यक है। इसके अतिरिक्त, सभी विरासत पीडी के लिए डेटा की खोज की जानी चाहिए और संग्रह के उद्देश्य के साथ मैप किया जाना चाहिए।

इसके अतिरिक्त, भविष्य में हम देखते हैं कि सहमति प्रबंधक डीपीडीपीए पारिस्थितिकी तंत्र में एक महत्वपूर्ण भूमिका निभा रहे हैं। इसलिए, डीएफ को यह सुनिश्चित करने के लिए अपना उचित परिश्रम करना चाहिए कि उनके द्वारा नियुक्त सहमति प्रबंधक डीपी की ओर से सहमति को प्रभावी और तकनीकी रूप से प्रबंधित करने में सक्षम हैं।

# अवधारणा 2: सहमति प्रबंधक

## 1. सहमति प्रबंधक कौन हैं?

डीपीडीपीए की धारा 2(जी) के अनुसार, सहमति प्रबंधक "डीपीबीआई के साथ पंजीकृत एक व्यक्ति है, जो एक सुलभ, पारदर्शी और अंतर-संचालन योग्य मंच के माध्यम से डीपी को अपनी सहमति देने, प्रबंधित करने, समीक्षा करने और वापस लेने में सक्षम बनाने के लिए एकल संपर्क बिंदु के रूप में कार्य करता है"।

डीपी सहमति प्रबंधक के माध्यम से अपनी सहमति दे सकते हैं, प्रबंधित कर सकते हैं, समीक्षा कर सकते हैं या वापस ले सकते हैं। दूसरे शब्दों में, डीएफ के लिए सहमति प्रबंधक की नियुक्ति अनिवार्य नहीं है। (धारा 6(7))। ऐसा सहमति प्रबंधक डीपी के प्रति उत्तरदायी रहेगा और उनकी ओर से कार्य करेगा (धारा 6(8))। इसके अतिरिक्त, सहमति प्रबंधक डीपीडीपीए (धारा 13(1)) के तहत पीडी या डीपी के अधिकारों से संबंधित उनके दायित्वों से संबंधित किसी भी कार्य या चूक के लिए डीपी (जहां लागू हो) को शिकायत निवारण प्रदान करेगा।

## 2. सहमति प्रबंधक के लिए कौन आवेदन कर सकता है?

डीपीडीपी नियमों के नियम 4 के अंतर्गत धारा 6(9) में यह प्रावधान है कि कोई भी भारतीय कंपनी डीपीबीआई में सहमति प्रबंधक के लिए आवेदन कर सकती है, बशर्ते कि ऐसी कंपनी:

- अपने दायित्वों को पूरा करने के लिए तकनीकी, परिचालन और वित्तीय दक्षता रखती है।
- कम से कम 20 मिलियन रुपये की कुल संपत्ति है।
- यह सुनिश्चित करती है कि उनकी वित्तीय स्थिति और प्रबंधन मजबूत है।
- यह सुनिश्चित करती है कि उनके व्यवसाय की परिमाण, पूंजी संरचना और आय की संभावनाएँ पर्याप्त हैं।
- यह सुनिश्चित करती है कि उनके संचालन में डीपी के हितों को सर्वोच्च प्राथमिकता दी जाए।
- यह सुनिश्चित करती है कि उनके चार्टर दस्तावेजों में "हितों के टकराव" से बचने के लिए प्रावधान शामिल हों।
- यह सुनिश्चित करती है कि उनके निदेशकों, प्रमुख प्रबंधकीय कर्मियों और वरिष्ठ प्रबंधन की निष्पक्षता और ईमानदारी की प्रतिष्ठा बनी रहे।
- प्रमाणित करती है कि (ए) उनका अंतर-संचालनीय प्लेटफ़ॉर्म डेटा सुरक्षा मानकों के अनुरूप है और (बी) तकनीकी तथा संगठनात्मक उपायों का अनुपालन करता है।

**पंजीकरण की शर्तों का उल्लंघन**

जहां सहमति प्रबंधक पंजीकरण की किसी भी शर्त का उल्लंघन करते हैं, वहां डीपीबीआई 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगा सकता है। (धारा 27(1)(डी))।

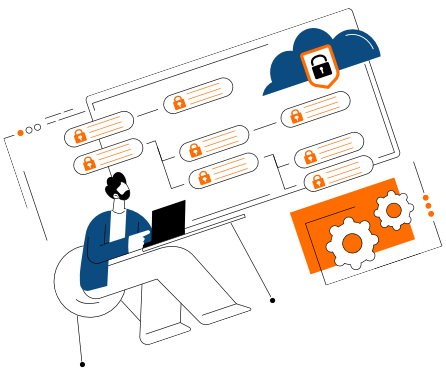
## 3. सहमति प्रबंधक के कर्तव्य क्या हैं?

**नियम 4 के अंतर्गत, सहमति प्रबंधक का कर्त्तव्य है:**

- अपने प्लेटफॉर्म का उपयोग करने वाले डीपी को या तो सीधे प्लेटफॉर्म पर शामिल डीएफ के माध्यम से या किसी अन्य डीएफ के माध्यम से सहमति देने में सक्षम बनाना, जो उनकी सहमति से डीपी के ऐसे पीडी को बनाए रखता है।
- सुनिश्चित करें कि साझा करते समय पीडी की सामग्री को पढ़ना कठिन हो।
- (ए) डीपी द्वारा प्रदान की गई, अस्वीकृत या वापस ली गई सहमति; (बी) सूचना; (सी) साझा किए गए डेटा का अभिलेख बनाए रखें।
- डीएफ के प्रमोटरों और प्रमुख प्रबंधकीय कर्मियों सहित डीएफ के साथ हितों के टकराव से बचें।
- अपने निदेशकों, प्रमुख प्रबंधकीय कर्मियों या वरिष्ठ प्रबंधन के डीएफ के साथ "हितों के टकराव" से बचने के लिए उपाय करें।
- डीपीडीपीए के अंतर्गत उप-अनुबंध या दायित्व का हस्तांतरण न करें और डेटा प्रोसेसिंग के लिए प्रत्ययी क्षमता में कार्य करें।
- डीपी के लिए सेवाओं तक पहुंच का मुख्य साधन एक वेबसाइट/ऐप बनाए रखना।
- कंपनी का नियंत्रण (बिक्री या विलय के माध्यम से) केवल डीपीबीआई की पूर्व स्वीकृति से ही स्थानांतरित किया जाए।
- सुरक्षा उपायों, निरंतर पंजीकरण और डीपीडीपीए अनुपालन को शामिल करने वाली लेखा परीक्षा और रिपोर्टिंग प्रणाली स्थापित करना।
- वेबसाइट/ऐप पर प्रमोटरों, निदेशकों, प्रमुख प्रबंधकीय कर्मियों, वरिष्ठ प्रबंधन और 2% शेयरधारिता वाले शेयरधारकों से संबंधित जानकारी प्रकाशित करें।

**दायित्वों का उल्लंघन**

सहमति प्रबंधक के दायित्वों के उल्लंघन के संबंध में डीपी द्वारा की गई शिकायत पर, डीपीबीआई जांच कर सकता है और 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगा सकता है। (धारा 27(1)(सी))।



## 4. चिंताएँ

**व्यावसायिक गतिविधियाँ:** यह स्पष्ट नहीं है कि सहमति प्रबंधक सहमति प्रबंधन सेवाएँ प्रदान करने के अलावा अन्य कार्य कर सकते हैं या नहीं। यह आवश्यक है कि वे अन्य व्यावसायिक गतिविधियाँ भी कर सकें, अन्यथा, वे आय के लिए पूरी तरह से डीएफ पर निर्भर रहेंगे, जिससे स्केलिंग में कठिनाई हो सकती है।

**पीडी की प्रोसेसिंग:** सहमति प्रबंधक पीडी सहित लेनदेन से संबंधित डेटा को प्रोसेस और स्टोर कर सकते हैं। यह स्पष्ट नहीं है कि क्या इससे वे स्वयं डीएफ बन सकते हैं।

**रद्दीकरण/निलंबन:** डीपीडीपी नियमों के नियम 4(5) के अनुसार, डीपीबी सहमति प्रबंधक के पंजीकरण को निलंबित या रद्द कर सकता है। इससे डीएफ के साथ व्यापार में अचानक बाधा उत्पन्न हो सकती है।

**हितों का टकराव:** नियम 4 को प्रथम अनुसूची के भाग बी के खंड 9 के साथ पढ़ने पर यह प्रावधान है कि सहमति प्रबंधक को डीएफ के साथ "हितों के टकराव" से बचना चाहिए। हालांकि, यह स्पष्ट नहीं करता है कि इसे प्लेटफ़ॉर्म पर शामिल डीएफ तक सीमित रखा जाना चाहिए या नहीं।

**इंटरऑपरेबल प्लेटफ़ॉर्म मानक:** आरबीआई के अकाउंट एग्रीगेटर ढांचे के विपरीत, जिसके लिए इंटरऑपरेबिलिटी मानकों पर विशिष्ट दिशा-निर्देश निर्धारित किए गए हैं, सहमति प्रबंधक के लिए ऐसे मानक निर्धारित नहीं किए गए हैं। हमारा मानना है कि समय आने पर कुछ तकनीकी मानक जारी किए जाएंगे।

**आगे बढ़ने का मार्ग**

हम आशा करते हैं कि डीपीडीपी पारिस्थितिकी तंत्र में सहमति प्रबंधक एक महत्वपूर्ण भूमिका निभाएंगे। इसके लिए आवश्यक है कि सहमति प्रबंधक अपने व्यवसाय के लिए केवल डीएफ पर निर्भर न रहें और एक स्वच्छ वातावरण में कार्य करें, जहां सभी पारदर्शिता और अंतर-संचालन मानकों को स्पष्ट रूप से परिभाषित किया गया हो।

# यदि "सहमति" पर ये जीडीपीआर मामले भारत में घटित होते हैं, तो क्या परिणाम होगा?

## जीडीपीआर के अंतर्गत सहमति क्या होती है?

अनुच्छेद 4(11) "सहमति" को डीएस की इच्छाओं के किसी भी स्वतंत्र, विशिष्ट, सूचित और स्पष्ट संकेत के रूप में परिभाषित करता है, जिसके माध्यम से वह एक बयान या स्पष्ट सकारात्मक कार्रवाई द्वारा अपने पीडी के प्रसंस्करण के लिए सहमति व्यक्त करता है।

अनुच्छेद 6(1)(ए) अनुच्छेद 7(1) के साथ सहमति को पीडी की प्रक्रिया के लिए कानूनी आधार के रूप में मान्यता प्रदान करता है, जिससे डीसी पर यह साबित करने की जिम्मेदारी आती है कि सहमति विधिवत प्राप्त की गई थी। इसके अतिरिक्त, अनुच्छेद 7(3) डीएस को किसी भी समय सहमति वापस लेने का अधिकार प्रदान करता है।

### 1. फ्रांस

- **पृष्ठभूमि:** लक्षित वेब विज्ञापन में विशेषज्ञता रखने वाली फ्रांसीसी कंपनी CRITEO ने व्यक्तिगत विज्ञापन प्रदर्शित करने के लिए कुकीज़ के माध्यम से अपने उपयोगकर्ताओं के ब्राउज़िंग व्यवहार को ट्रैक किया। 8 नवंबर, 2018 को, "प्राइवेसी इंटरनेशनल" नामक एक संघ ने फ्रांसीसी डेटा सुरक्षा प्राधिकरण, यानी कमीशन नेशनले डे ल'इंफॉर्मेटिक एट डेस लिबर्टीज (CNIL) के समक्ष शिकायत दर्ज की, जिसमें आरोप लगाया गया कि व्यक्तिगत डेटा को कानूनी रूप से संसाधित नहीं किया गया था। 4 दिसंबर, 2018 को "नन ऑफ़ योर बिज़नेस" नामक एक संघ द्वारा दूसरी शिकायत प्रस्तुत की गई, जिसमें यह दावा किया गया कि उपयोगकर्ताओं को डेटा प्रोसेसिंग के लिए अपनी सहमति/आपत्ति वापस लेने की अनुमति नहीं थी।

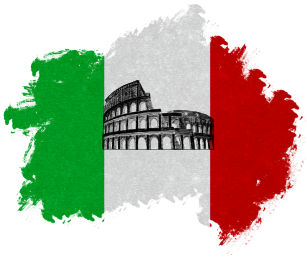
- **निष्कर्ष:** CNIL ने यह निष्कर्ष निकाला कि CRITEO ने जीडीपीआर के अनुच्छेद 6(1)(a) और 7(1) के तहत प्रसंस्करण के लिए वैध उपयोगकर्ता सहमति प्राप्त करने में असफलता दिखाई। इसके अतिरिक्त, अनुच्छेद 7(3) के तहत आवश्यक सहमति वापसी तंत्र प्रभावी नहीं था। परिणामस्वरूप, CNIL ने 15 जून, 2023 को CRITEO पर 40 मिलियन यूरो या लगभग 45 मिलियन अमेरिकी डॉलर का जुर्माना लगाया।

## भारत में क्या होगा?

- **प्रासंगिक डीपीडीपीए प्रावधान:** धारा 4(1) धारा 6(1) के साथ यह निर्धारित करती है कि पीडी की प्रोसेसिंग सहमति के आधार पर की जा सकती है, जो स्वतंत्र, सूचित, विशिष्ट, बिना शर्त और स्पष्ट हो। धारा 6(4) यह भी स्पष्ट करती है कि यदि सहमति प्रोसेसिंग का आधार है, तो डीपी किसी भी समय अपनी सहमति वापस ले सकता है, उसी सरलता से जैसे कि इसे प्रदान किया गया था। इसके अतिरिक्त, धारा 8(7) के अनुसार, सहमति वापस लेने पर डेटा को हटा दिया जाना चाहिए, जब तक कि इसे कानूनी रूप से बनाए रखना आवश्यक न हो।

- **जुर्माना:** पर्याप्त सहमति प्राप्त करने में विफलता, वापसी विकल्प प्रदान न करने, या पीडी को हटाने में विफलता के परिणामस्वरूप प्रत्येक उल्लंघन के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर का जुर्माना लगाया जा सकता है, और सामूहिक रूप से 1.5 बिलियन रुपये या लगभग 18 मिलियन अमेरिकी डॉलर का जुर्माना लगाया जा सकता है।

## 2. इटली



- **पृष्ठभूमि:** कई उपयोगकर्ताओं ने मोबाइल, फिक्स्ड-लाइन, ब्रॉडबैंड और आईटी सेवाएं प्रदान करने वाली दूरसंचार प्रदाता विंड ट्रे स्पा के खिलाफ शिकायतें दर्ज की, जिसमें आरोप लगाया गया कि वे स्पष्ट उपयोगकर्ता सहमति प्राप्त किए बिना फोन कॉल, एसएमएस, ई-मेल, फैक्स आदि के माध्यम से प्रचार संचार भेज रहे थे। यह भी आरोप लगाया गया कि सहमति या आपत्ति वापस लेने के बाद भी ये संचार जारी रहे। इसके अतिरिक्त, विंड ट्रे ने दो एप्लिकेशन संचालित किए, जिनका नाम माईविंड और माई3 मोबाइल था। इन एप्लिकेशनों में प्रत्येक लॉगिन पर मार्केटिंग, प्रोफाइलिंग, थर्ड-पार्टी संचार आदि के लिए सहमति की आवश्यकता होती थी और अगले 24 घंटों तक सहमति वापस लेने की अनुमति नहीं होती थी।

- **निष्कर्ष:** इतालवी डेटा सुरक्षा प्राधिकरण, जिसे गैरेंटे पर ला प्रोटेज़ियोन देई डेटा पर्सोनाली (गारंटे) के नाम से जाना जाता है, ने यह निष्कर्ष निकाला कि प्रचार संचार वैध उपयोगकर्ता सहमति के बिना भेजे गए थे। इसके अतिरिक्त, माईविंड और माई3 ऐप ने उपयोगकर्ताओं को 24 घंटे तक सहमति वापस लेने की अनुमति न देकर उपयोगकर्ता अधिकारों में बाधा उत्पन्न की। इन कार्रवाइयों को अनुच्छेद 6(1)(ए), 7(3) और 21 (आपत्ति का अधिकार) के साथ गैर-अनुपालन के रूप में माना गया। परिणामस्वरूप, 9 जुलाई, 2020 को 17 मिलियन यूरो या लगभग 19 मिलियन अमेरिकी डॉलर का जुर्माना लगाया गया।

### भारत में क्या होगा?

- **प्रासंगिक डीपीडीपीए प्रावधान:** धारा 6(1) के अनुसार, सहमति डेटा प्रोसेसिंग के उद्देश्य तक सीमित रहनी चाहिए। इसके अतिरिक्त, धारा 6(4) आर/डब्ल्यू धारा 8(7)(ए) डीपी को किसी भी समय अपनी सहमति वापस लेने की अनुमति देती है, और सहमति वापस लेने पर डीएफ को व्यक्तिगत डेटा को मिटाने की आवश्यकता होती है, जब तक कि प्रतिधारण कानूनी रूप से आवश्यक न हो।

- **जुर्माना:** स्पष्ट सहमति प्राप्त करने में विफलता/सहमति वापसी विकल्प प्रदान करने में विफलता/पीडी को न मिटाने पर प्रत्येक के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है। संयुक्त रूप से, इन उल्लंघनों पर 1.5 बिलियन रुपये या लगभग 18 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है।

## 3. स्पेन

- **पृष्ठभूमि:** कैक्साबैंक एस.ए., एक वित्तीय संस्थान, पर एक क्रेडिट स्कोरिंग कंपनी के साथ प्रोफाइलिंग के उद्देश्य से एक ग्राहक का डेटा साझा करने का आरोप लगाया गया, जिसमें आईडी नंबर, जन्म तिथि, आय, वेतन, रोजगार आदि शामिल था, जबकि 2014 में उनका बैंकिंग संबंध समाप्त हो चुका था।

- **निष्कर्ष:** स्पेनिश डेटा सुरक्षा प्राधिकरण, जिसे एजेंसिया एस्पानोला डे प्रोटेक्शन डे डेटास (AEPD) के नाम से जाना जाता है, ने यह निष्कर्ष निकाला कि कैक्साबैंक वैध सहमति प्राप्त करने में असफल रहा। प्राप्त सहमति न तो सूचित थी और न ही विशिष्ट, क्योंकि उपयोगकर्ता प्रत्येक प्रसंस्करण उद्देश्य के लिए विस्तृत स्वीकृति नहीं दे सकते थे। कैक्साबैंक की गोपनीयता नीति में उपयोग किए जा रहे विशिष्ट डेटा, प्रोफाइलिंग की सीमा, और तीसरे पक्ष के विपणन या पूर्व-स्वीकृत क्रेडिट ऑफ़र प्राप्त करने की क्षमता पर स्पष्टता का अभाव था। इसके अतिरिक्त, डेटा को वैध अनुबंध के बिना प्रोफाइलिंग संस्थाओं के साथ साझा किया गया था। इसे अनुच्छेद 4(11), 6(1)(ए), 7(1), और 28(3) (प्रोसेसर अनुबंध) का उल्लंघन माना गया और 10 अक्टूबर, 2021 को 3 मिलियन यूरो या लगभग 3 मिलियन अमेरिकी डॉलर का जुर्माना लगाया गया।

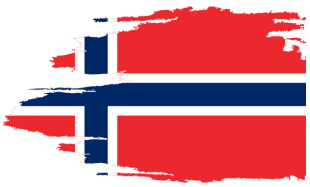
**भारत में क्या होगा?**

- **प्रासंगिक डीपीडीपीए प्रावधान:** धारा 6(1) के अंतर्गत, सहमति स्वतंत्र, सूचित, विशिष्ट, बिना शर्त और स्पष्ट होनी चाहिए। धारा 8(2) के अनुसार, जब कोई डीएफ अपनी ओर से डेटा प्रोसेस करने के लिए डीपीआर को नियुक्त करता है, तो यह वैध अनुबंध के तहत होना चाहिए। इसके अतिरिक्त, धारा 8(7) के अनुसार, निर्दिष्ट उद्देश्य की पूर्ति के बाद, डीएफ को डेटा को मिटाना चाहिए और यह सुनिश्चित करना चाहिए कि उसके प्रोसेसर भी ऐसा ही करें, जब तक कि कानून द्वारा डेटा को बनाए रखना आवश्यक न हो।

- **जुर्माना:** वैध सहमति प्राप्त न करने, उचित अनुबंध के बिना प्रोसेसर को नियुक्त करने, या पीडी को मिटाने में विफल रहने पर प्रत्येक उल्लंघन के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है। कुल जुर्माना 1.5 बिलियन रुपये या लगभग 18 मिलियन अमेरिकी डॉलर तक हो सकता है।

## 4. नॉर्वे

- **पृष्ठभूमि:** ग्रिंडर एलएलसी, एक अमेरिकी कंपनी, एक जीपीएस-आधारित सोशल नेटवर्किंग ऐप का संचालन करती थी। 14 जनवरी, 2020 को, नॉर्वेजियन डेटा प्रोटेक्शन अथॉरिटी, जिसे डेटाटिल्सिनेट कहा जाता है, ने नॉर्वेजियन कंज्यूमर काउंसिल (एनसीसी) से 3 शिकायतें प्राप्त कीं, जिसमें आरोप लगाया गया कि ग्रिंडर ने अपने विज्ञापन भागीदारों के साथ अवैध रूप से डेटा साझा किया। इसके अतिरिक्त, ग्रिंडर की सहमति तंत्र के तहत उपयोगकर्ताओं को "आगे बढ़ें" पर क्लिक करके गोपनीयता नीति को स्वीकार करना आवश्यक था, जिसके बाद "मैं गोपनीयता नीति स्वीकार करता हूं" का विकल्प था। यदि उपयोगकर्ता "रद्द करें" का चयन करते हैं, तो ऐप तक पहुंच से इनकार कर दिया जाता है।



- **निष्कर्ष:** जांच के पश्चात, यह स्पष्ट हुआ कि ग्रिंडर ने अपने विज्ञापन भागीदारों के साथ पहचान संबंधी विवरण, पता, उपकरण की जानकारी, आयु, लिंग आदि जैसी व्यक्तिगत डेटा साझा की। इसके अतिरिक्त, ग्रिंडर की सहमति प्रणाली सभी प्रसंस्करण गतिविधियों के लिए समग्र सहमति पर निर्भर थी, जिससे उपयोगकर्ताओं को विशिष्ट उद्देश्यों को स्वीकार या अस्वीकार करने की अनुमति नहीं थी। यह अनुच्छेद 4(11), 6(1)(ए) और अनुच्छेद 7(1) का उल्लंघन करता है। डेटाटिल्सिनेट ने यह भी निष्कर्ष निकाला कि ग्रिंडर ने सहमति वापस लेना कठिन बना दिया, जिससे उपयोगकर्ताओं को उपकरण-स्तरीय सेटिंग्स में परिवर्तन करने या ऐप के प्रीमियम संस्करण की सदस्यता लेने की आवश्यकता होती है, जो अनुच्छेद 7(3) का उल्लंघन करता है। परिणामस्वरूप, 13 दिसंबर, 2021 को कुल 6.5 मिलियन यूरो या लगभग 7 मिलियन अमेरिकी डॉलर का जुर्माना लगाया गया।

**भारत में क्या होगा?**

- **प्रासंगिक डीपीडीपीए प्रावधान:** धारा 6(1) के अनुसार सहमति विशिष्ट और बिना शर्त होनी चाहिए। इसके अतिरिक्त, धारा 6(4) में यह प्रावधान है कि यदि सहमति प्रक्रिया का आधार है, तो डीपी किसी भी समय सहमति को वापस ले सकता है, उतनी ही सरलता से जितनी सरलता से सहमति दी गई थी।

- **जुर्माना:** पर्याप्त सहमति प्राप्त न करने या वापसी का विकल्प न देने पर प्रत्येक उल्लंघन के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर का जुर्माना तथा सामूहिक रूप से 1 बिलियन रुपये या लगभग 12 मिलियन अमेरिकी डॉलर का जुर्माना लगाया जा सकता है।

## 5. पोलैंड

- **पृष्ठभूमि:** डेटा प्रोसेसिंग, होस्टिंग और संबंधित सेवाओं में संलग्न पोलिश कंपनी ClickQuickNow पर आरोप लगाया गया है कि वह डीपी द्वारा सहमति वापस लेने या डेटा मिटाने के अनुरोधों में बाधाएं उत्पन्न कर रही थी।

- **निष्कर्ष:** शिकायतों की जांच के दौरान, पोलिश डेटा सुरक्षा प्राधिकरण, उर्जाद ओक्रोनी डैनिच ओसोबोविक (यूओडीओ), ने यह निष्कर्ष निकाला कि ClickQuickNow व्यक्तियों को आसानी से सहमति वापस लेने (अनुच्छेद 7(3)) और मिटाने के अपने अधिकार का प्रयोग करने (अनुच्छेद 17) के लिए आवश्यक तकनीकी और संगठनात्मक उपायों को लागू करने में असफल रहा। इन उल्लंघनों के परिणामस्वरूप, 10 फरवरी, 2021 को 47,000 यूरो या लगभग 53,000 अमेरिकी डॉलर का जुर्माना लगाया गया।

**भारत में क्या होगा?**

- **प्रासंगिक डीपीडीपीए प्रावधान:** धारा 6(4) में यह उल्लेखित है कि यदि डीपी द्वारा दी गई सहमति प्रसंस्करण का आधार है, तो इसे उसी सरलता से वापस लिया जा सकता है जिस सरलता से इसे प्रदान किया गया था। इसके अतिरिक्त, धारा 8(4) के अनुसार, डीएफ को डीपीडीपीए के प्रावधानों का प्रभावी अनुपालन सुनिश्चित करने के लिए उचित तकनीकी और संगठनात्मक उपायों को लागू करना आवश्यक है। इसके अलावा, धारा 8(7) में कहा गया है कि डीपीओ को डीपी द्वारा अपनी सहमति वापस लेने या उद्देश्य की पूर्ति पर पीडी को मिटा देना चाहिए, जब तक कि कानून के अनुसार प्रतिधारण की आवश्यकता न हो।

- **जुर्माना:** उचित निकासी तंत्र प्रदान करने में विफलता, उचित तकनीकी और संगठनात्मक उपायों को लागू न करने, या डेटा को न मिटाने पर प्रत्येक उल्लंघन के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर का जुर्माना लगाया जा सकता है, और सामूहिक रूप से कुल जुर्माना 1.5 बिलियन रुपये या लगभग 18 मिलियन अमेरिकी डॉलर तक हो सकता है।

## 6. लक्ज़मबर्ग

- **पृष्ठभूमि:** 2021 में 10,000 व्यक्तियों की ओर से फ्रांसीसी एनजीओ "ला क्वाड्रैचर डू नेट" द्वारा लक्ज़मबर्ग के डेटा संरक्षण प्राधिकरण यानी कमीशन नेशनेल पोर ला प्रोटेक्शन डेस डोननेस (सीएनपीडी) के साथ एक सामूहिक शिकायत दर्ज की गई थी, जिसमें आरोप लगाया गया था कि अमेज़ॅन यूरोप कोर एसएआरएल की लक्षित विज्ञापन प्रथाएं वैध, स्वतंत्र रूप से प्राप्त सहमति पर आधारित नहीं थीं।

- **निष्कर्ष:** यद्यपि पेशेवर गोपनीयता दायित्वों के कारण संपूर्ण तर्क गोपनीय रखा गया है, CNPD ने यह निष्कर्ष निकाला कि अमेज़ॅन यूरोप कोर एसएआरएल के लक्षित विज्ञापन ने अनुच्छेद 6(1)(a) और 7(1) के अंतर्गत जीडीपीआर सहमति आवश्यकताओं का उल्लंघन किया है। परिणामस्वरूप, 18 मार्च, 2025 को 746 मिलियन यूरो या लगभग 845 मिलियन अमेरिकी डॉलर का जुर्माना लगाया गया। इसके अतिरिक्त, अमेज़ॅन ने इस निर्णय के खिलाफ अपील दायर की, जिसे लक्ज़मबर्ग के प्रशासनिक न्यायालय ने खारिज कर दिया।

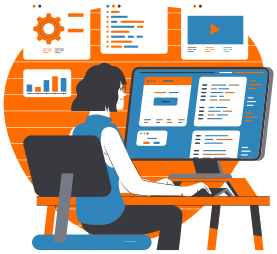
### भारत में क्या होगा?

- **प्रासंगिक डीपीडीपीए प्रावधान:** जैसा कि उल्लेखित है, धारा 6(1) के अनुसार प्रसंस्करण स्वतंत्र, सूचित, विशिष्ट, बिना शर्त और स्पष्ट सहमति पर निर्भर होना चाहिए। धारा 6(4) के अनुसार, डीपी दी गई सहमति को वापस ले सकता है।

- **जुर्माना:** पर्याप्त सहमति प्राप्त करने में विफलता या उचित वापसी तंत्र उपलब्ध न कराने पर, प्रत्येक उल्लंघन के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर का जुर्माना लगाया जा सकता है, और कुल जुर्माना 1 बिलियन रुपये या लगभग 12 मिलियन अमेरिकी डॉलर हो सकता है।

# अवधारणा 3: महत्वपूर्ण डेटा फिड्यूसरी

## 1. एसडीएफ कौन है?



डीपीडीपीए के अंतर्गत, एसडीएफ, डीएफ की एक उपश्रेणी मानी जाती है।

डीपीडीपीए की धारा 2(जेड) एसडीएफ को "किसी भी डीएफ या डीएफ के वर्ग के रूप में परिभाषित करती है, जिसे धारा 10 के अंतर्गत केंद्र सरकार द्वारा अधिसूचित किया जा सकता है।"

## 2. एसडीएफ का निर्धारण किस प्रकार किया जाता है?

डीपीडीपीए की धारा 10(1) के अनुसार, एक डीएफ या डीएफ के वर्ग को निम्नलिखित कारकों के आधार पर एसडीएफ के रूप में अधिसूचित किया जा सकता है:

- संवेदनशीलता और संसाधित पीडी की मात्रा
- डीपी अधिकारों के लिए जोखिम
- भारत की संप्रभुता और अखंडता पर संभावित प्रभाव
- चुनावी लोकतंत्र, राज्य सुरक्षा और सार्वजनिक व्यवस्था के लिए खतरा

## 3. एसडीएफ की अनुपालन आवश्यकताएँ क्या हैं?

- **डीपीओ की नियुक्ति:** एसडीएफ को भारत में अपने प्रतिनिधित्व के लिए एक डीपीओ नामित करना चाहिए। यह डीपीओ निदेशक मंडल के प्रति उत्तरदायी होगा और डीपीडीपीए के तहत शिकायत निवारण संपर्क बिंदु के रूप में कार्य करेगा। (धारा 10(2)(ए))
- **स्वतंत्र डेटा ऑडिटर की नियुक्ति:** ऐसे ऑडिटर को डेटा ऑडिट करने और डीपीडीपीए के साथ एसडीएफ के अनुपालन का मूल्यांकन करने के लिए नियुक्त किया जाना चाहिए। (धारा 10(2)(बी))
- **डीपीआईए और आवधिक ऑडिट का आयोजन:** एसडीएफ को डीपीडीपीए और डीपीडीपी नियमों के अनुपालन को सुनिश्चित करने के लिए वार्षिक डीपीआईए और ऑडिट का आयोजन करना चाहिए। महत्वपूर्ण टिप्पणियों का सारांश भी डीपीबीआई को प्रस्तुत किया जाना चाहिए। (धारा 10(2)(सी)(i) और (ii) तथा नियम 12(1) और (2))
- **एल्गोरिदमिक सॉफ्टवेयर:** एसडीएफ को यह सुनिश्चित करने के लिए "उचित परिश्रम" करना चाहिए कि उनके द्वारा तैनात "एल्गोरिदमिक सॉफ्टवेयर" डीपी के अधिकारों के लिए कोई जोखिम उत्पन्न नहीं करता है। (नियम 12(3))
- **डेटा स्थानांतरण प्रतिबंध:** एसडीएफ को यह सुनिश्चित करना होगा कि समिति की सिफारिशों के आधार पर सीजी द्वारा निर्दिष्ट पीडी और "इसके प्रवाह से संबंधित यातायात डेटा" भारत के बाहर स्थानांतरित नहीं किया जाए। (नियम 12(4))

PSA
LEGAL COUNSELLORS

### 4. यदि एसडीएफ के अनुपालन में विफलता होती है, तो क्या परिणाम होगा?

डीपीडीपीए की अनुसूची के अनुसार धारा 33(1) के तहत, यदि डीपीबी जांच के उपरांत इस निष्कर्ष पर पहुंचता है कि एसडीएफ धारा 10(2) के तहत अपने दायित्वों का पालन करने में असफल रहे हैं, तो वह 1.5 बिलियन रुपये या लगभग 18 मिलियन अमेरिकी डॉलर तक का जुर्माना लगा सकता है।

### 5. मुद्दे

- **परिभाषित थ्रेसहोल्ड की अनुपस्थिति:** डीएफ को एसडीएफ के रूप में अधिसूचित करना "प्रसंस्कृत पीडी की मात्रा और संवेदनशीलता" जैसे कारकों पर निर्भर करता है, लेकिन कोई स्पष्ट थ्रेसहोल्ड निर्धारित नहीं किया गया है। इसके अतिरिक्त, नियम 22(1) केंद्र सरकार डीएफ से जानकारी प्राप्त करने की अनुमति देता है ताकि यह निर्धारित किया जा सके कि उन्हें एसडीएफ के रूप में अधिसूचित किया जाना चाहिए या नहीं। इसका तात्पर्य है कि किसी भी डीएफ या डीएफ के वर्ग को किसी भी समय एसडीएफ के रूप में अधिसूचित किया जा सकता है।
- **डेटा स्थानीयकरण का अप्रत्यक्ष रूप:** नियम 12(4) के अनुसार एसडीएफ को कुछ निश्चित पीडी (जैसा कि केंद्र सरकार द्वारा गठित समिति द्वारा निर्दिष्ट किया गया है) और भारत के भीतर इसके प्रवाह से संबंधित यातायात डेटा को रखने के लिए उपाय करने की आवश्यकता है। यह एसडीएफ के लिए परिचालन और तकनीकी चुनौतियाँ उत्पन्न कर सकता है। इसके अतिरिक्त, यह स्पष्ट नहीं है कि स्थानीयकरण पर यह प्रतिबंध केवल एसडीएफ पर ही क्यों लागू होता है और डीएफ पर क्यों नहीं। आगे बढ़ते हुए, यह संभावना है कि यदि कोई डीएफ डेटा को संसाधित करता है जिसे केंद्र सरकार को नियम 12(4) के अनुसार स्थानीयकृत करने की आवश्यकता होती है, तो ऐसे डीएफ को एसडीएफ के रूप में अधिसूचित किया जा सकता है।
- **एल्गोरिदमिक सॉफ़्टवेयर के लिए उचित परिश्रम:** डीपीडीपी नियमों के अनुसार, एसडीएफ को उनके द्वारा तैनात किए गए किसी भी "एल्गोरिदमिक सॉफ़्टवेयर" के लिए उचित परिश्रम करना अनिवार्य है। हालाँकि, यह ध्यान में रखते हुए कि आज लगभग सभी सॉफ़्टवेयर किसी न किसी रूप में एल्गोरिदम का उपयोग करते हैं, इससे परिचालन अक्षमताएँ उत्पन्न हो सकती हैं और तैनाती की समयसीमा पर प्रभाव पड़ सकता है। इसके अतिरिक्त, उन्हें अनुपालन प्रदर्शित करने के लिए ऑडिट ट्रेल बनाए रखने की आवश्यकता हो सकती है।
- **अनुपालन की लागत:** यदि मध्यम/छोटे डीएफ को एसडीएफ के रूप में अधिसूचित किया जाता है, तो उनके अनुपालन की लागत में उल्लेखनीय वृद्धि होगी। जबकि बड़ी कंपनियां इन खर्चों का प्रबंधन कर सकती हैं, छोटे डीएफ को विनियामक दायित्वों को पूरा करने में गंभीर वित्तीय दबाव का सामना करना पड़ सकता है।
- **डीपीआईए और ऑडिट:** एसडीएफ को हर वर्ष डीपीआईए आयोजित करने की आवश्यकता होती है, भले ही वे कोई नया सॉफ़्टवेयर लागू न करें या प्रोसेसिंग गतिविधियों में कोई परिवर्तन न करें, यह अनावश्यक और बोझिल हो सकता है। आदर्श रूप से, डीपीआईए तब आयोजित किया जाना चाहिए जब डेटा संसाधित करने के तरीके में कोई परिवर्तन हो।

**आगे बढ़ने का मार्ग**

चूंकि गैर-अनुपालन के लिए कोई महत्वपूर्ण दंड नहीं है, इसलिए उच्च मात्रा/संवेदनशील पीडी को संसाधित करने वाले डीएफ को नियामक आवश्यकताओं के अनुपालन को सुनिश्चित करने के लिए सक्रिय रूप से अंतर का आकलन करना चाहिए, विशेष रूप से तब जब केंद्र सरकार के पास उन्हें एसडीएफ के रूप में अधिसूचित करने का अधिकार है।

# अवधारणा 4: फिड्युशियरी-प्रोसेसर संबंध का प्रबंधन करना

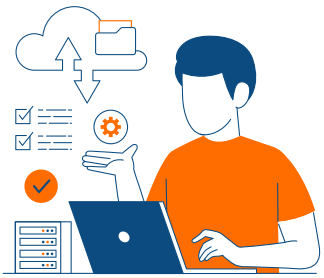
## 1. प्रसंस्करण क्या है?

प्रसंस्करण डिजिटल पीडी पर किया जाने वाला संपूर्ण या आंशिक स्वचालित संचालन या संचालन का समूह है। इसमें "संग्रह, रिकॉर्डिंग, संगठन, संरचना, भंडारण, अनुकूलन, पुनर्प्राप्ति, उपयोग, संरेखण या संयोजन, अनुक्रमण, साझाकरण, संचरण द्वारा प्रकटीकरण, प्रसार या अन्यथा उपलब्ध कराना, प्रतिबंध, विलोपन या विनाश जैसे संचालन शामिल हैं" (धारा 2(x))।

**डीएफ और डीपीआर कौन हैं?**

डीएफ का अर्थ है "कोई भी व्यक्ति जो अकेले या अन्य व्यक्तियों के साथ मिलकर पीडी के प्रसंस्करण के उद्देश्य और साधन निर्धारित करता है" (धारा 2(*i*))। इसके अतिरिक्त, डीपीआर का अर्थ है "कोई भी व्यक्ति जो डीएफ की ओर से पीडी का प्रसंस्करण करता है" (धारा 2(के))। डेटा प्रोसेसर को केवल वैध अनुबंधों के तहत नियुक्त किया जाना चाहिए (धारा 8(2))।

## 2. डीएफ के उत्तरदायित्व क्या हैं?



- डीपीडीपीए और मसौदा नियमों का अनुपालन करें (धारा 8(1))
- एक वैध अनुबंध के अंतर्गत अपनी ओर से पीडी को संसाधित करने के लिए एक डीपीआर (यदि आवश्यक हो) की नियुक्ति करें (धारा 8(2))
- निर्णय लेने के लिए उपयोग किए जाने वाले पीडी की संपूर्णता, सटीकता और स्थिरता सुनिश्चित करें/जब किसी अन्य डेटा फिड्युसरी को इसका प्रकटीकरण किया जाता है (धारा 8(3))
- उचित तकनीकी और संगठनात्मक उपायों को लागू करना (धारा 8(4))
- एन्क्रिप्शन, मास्किंग आदि जैसे उपयुक्त सुरक्षा उपायों के माध्यम से अपने या डीपीआर के अधीन पीडी की सुरक्षा करें (धारा 8(5) नियम 6(1)(ए) के अनुसार)
- डीपीबीआई और प्रभावित डीपी को पीडी उल्लंघन की सूचना प्रदान करें (धारा 8(6))
- जब तक कानून द्वारा अपेक्षित न हो, सहमति वापस लेने या निर्दिष्ट उद्देश्य की पूर्ति पर व्यक्तिगत डेटा को मिटाने या अपने प्रोसेसरों से हटाने का कारण बनना (धारा 8(7))
- डीपीओ या अधिकृत कार्मिक की संपर्क जानकारी अपनी वेबसाइट या ऐप पर प्रकाशित करें (धारा 8(9) नियम 9 के अनुसार)
- डीपी के लिए एक सक्षम शिकायत निवारण तंत्र स्थापित करें (धारा 8(10))

**डीएफ के संदर्भ में अनुमान**

डीपीडीपीए के तहत किसी भी उल्लंघन या गैर-अनुपालन के लिए डीएफ पूरी तरह से उत्तरदायी हैं। ऐसा प्रतीत होता है कि यह इस आधार पर किया गया है कि डीएफ डीपीआर के साथ अपने समझौतों पर बातचीत करने की स्थिति में होंगे। यह हमेशा संभव नहीं हो सकता, क्योंकि कुछ प्रोसेसर (जैसे क्लाउड सेवा प्रदाता) बिना किसी अनुबंध वार्ता के खाता बनाकर शामिल हो जाते हैं।

## 3. डीएफ को डीपीआर से कौन से प्रश्न पूछने चाहिए?


- क्या आप पीडी को किसी अन्य उद्देश्य के लिए संसाधित करते हैं?
- यदि निर्देश दिया जाए तो आप प्रसंस्करण कैसे समाप्त करेंगे? इसे सुनिश्चित करने के लिए कौन से उपाय किए गए हैं?
- आप डेटा संरक्षण और विलोपन आवश्यकताओं का पालन कैसे करते हैं?
- क्या आप उप-प्रसंस्करणकर्ताओं को नियुक्त करते हैं? यदि हाँ, तो क्या उन्हें पूर्व अनुमोदन के साथ और समान दायित्वों वाले अनुबंधों के अंतर्गत नियुक्त किया जाता है?
- क्या आपके पास कोई दस्तावेजीकृत सूचना सुरक्षा नीति है? इसे सभी टीमों में किस प्रकार लागू किया जाता है?
- क्या आप भारत के बाहर डेटा स्थानांतरित करते हैं?
- आप यह कैसे सुनिश्चित करते हैं कि केवल अधिकृत व्यक्ति ही पीडी तक पहुंच पाएं? क्या आप अद्वितीय उपयोगकर्ता खाते, बहु-कारक प्रमाणीकरण आदि का उपयोग करते हैं?
- क्या आप स्टोरेज और ट्रांज़िट के दौरान पीडी को एन्क्रिप्ट करते हैं? यदि हाँ, तो क्या आप किसी उद्योग-मानक प्रोटोकॉल (जैसे, HTTPS/TLS RFC 2818/8446) का उपयोग करते हैं?
- क्या आपने SOC 2, NIST, या ISO 27001 जैसे सुरक्षा मानकों को लागू किया है?
- क्या आपके पास घटना प्रतिक्रिया नीति का एक दस्तावेज है जिसमें पीडी उल्लंघन के मामलों में की जाने वाली कार्रवाई की रूपरेखा प्रस्तुत की गई है? क्या आपके पास इसके लिए कोई बीमा कवरेज उपलब्ध है?
- क्या आप अपने कर्मचारियों, सलाहकारों या साझेदारों के लिए डेटा प्रबंधन या घटना प्रबंधन जैसे विषयों पर सुरक्षा जागरूकता प्रशिक्षण आयोजित करते हैं?
- क्या आप किसी तृतीय पक्ष के उपकरण का उपयोग करते हैं जो अधिक प्रभावी लेखा परीक्षा परिश्रम तंत्र की अनुमति देता है?

**डीएफ को क्या करना चाहिए?**

यह देखते हुए कि डीएफ पूरी तरह से डीपीडीपीए के तहत उत्तरदायी है, यह आवश्यक है कि इसकी कानूनी, सूचना सुरक्षा और आईटी टीमें डीपीआर के साथ अपने संबंध को औपचारिक रूप देते हुए समन्वयित रूप से कार्य करें। इसके अतिरिक्त, डीएफ को न्यूनतम मानकों (जैसे, डेटा सुरक्षा प्रथाएँ, अनुपालन इतिहास, वित्तीय स्थिरता, उल्लंघन प्रतिक्रिया क्षमताएँ आदि) को रेखांकित करते हुए एक आंतरिक जोखिम मीट्रिक स्थापित करना चाहिए, जिसे डीपीआर को पूरा करना आवश्यक है।

## 4. डीपीए के कुछ महत्वपूर्ण खंड कौन से हैं?


- **प्रसंस्करण का दायरा:** संसाधित किए जाने वाले पी.डी. की श्रेणियों, प्रसंस्करण के उद्देश्य, की जाने वाली प्रसंस्करण गतिविधियों और प्रसंस्करण की अवधि को परिभाषित करता है।
- **उद्देश्य सीमा:** पी.डी. को किसी अन्य द्वितीयक उद्देश्य के लिए संसाधित नहीं किया जाएगा, जब तक कि अन्यथा सहमति न दी गई हो।
- **डीपी के दायित्व:** डेटा संरक्षण कानूनों के अनुपालन में पीडी को संसाधित करने सहित डीपीआर के लिए राज्य की जिम्मेदारियाँ।
- **समर्थन:** डीपीआर को सभी आवश्यक संसाधन उपलब्ध कराने की आवश्यकता है, जिसमें लॉग और अन्य दस्तावेज शामिल हैं, लेकिन इन्हीं तक सीमित नहीं हैं, समय पर और प्रभावी ढंग से जब भी आवश्यकता हो। इसके अतिरिक्त, उन्हें अपने कानूनी दायित्वों को पूरा करने में डीएफ के साथ सहयोग करना चाहिए।

- **डेटा प्रतिधारण और विलोपन:** डीपीआर को निर्दिष्ट उद्देश्य की पूर्ति पर या डीएफ द्वारा निर्देशित किए जाने पर पीडी को हटाने की आवश्यकता होती है, जब तक कि प्रतिधारण कानून द्वारा अनिवार्य न हो।
- **डेटा सुरक्षा:** डीपीआर को उपयुक्त तकनीकी और संगठनात्मक उपायों को लागू करना चाहिए और डेटा सुरक्षा के संरक्षण के लिए उचित सुरक्षा उपाय करने चाहिए।
- **डेटा अद्यतनीकरण:** डीपीआर को डीएफ द्वारा सूचित करने पर पीडी को अद्यतन, सुधार या पूर्ण करना।
- **डेटा उल्लंघन:** डीपीआर द्वारा सभी पीडी उल्लंघनों की तात्कालिकता से डीएफ को रिपोर्ट की जानी चाहिए। इसके अतिरिक्त, उल्लंघन की स्थिति में डीपीआर को सहायता प्रदान करनी चाहिए।
- **लेखापरीक्षा अधिकार:** डीएफ के पास डीपीआर के अनुपालन को सुनिश्चित करने के लिए लेखापरीक्षा अधिकार होंगे।
- **गोपनीयता:** सभी प्राप्त पीडी को गोपनीय माना जाएगा और केवल आवश्यकता पड़ने पर ही इसका खुलासा किया जाएगा।
- **क्षतिपूर्ति:** डीपीआर को (क) अपने दायित्वों के उल्लंघन, (ख) उचित सुरक्षा उपायों को लागू करने में विफलता, (ग) अपने कार्यों या चूक के कारण उत्पन्न होने वाले पीडी उल्लंघनों, (घ) डेटा प्रतिधारण या विलोपन आवश्यकताओं का पालन करने में विफलता से उत्पन्न किसी भी हानि/क्षति के लिए डीएफ को क्षतिपूर्ति करनी होगी।
- **उप-प्रसंस्करणकर्ताओं का उपयोग:** डीएफ की पूर्व लिखित स्वीकृति के बिना उप-प्रसंस्करणकर्ताओं की नियुक्ति निषिद्ध है। उप-प्रसंस्करणकर्ताओं को केवल समान दायित्वों वाले वैध अनुबंधों के अंतर्गत नियुक्त किया जाएगा।
- **सीमा-पार डेटा स्थानांतरण:** सीमा-पार स्थानांतरण डीएफ की पूर्व लिखित सहमति के साथ और डेटा संरक्षण कानूनों के अनुपालन में किया जाएगा।

**डीपीआर का मूल्यांकन**

डीपीडीपीए डीएफ पर 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर से लेकर 2.5 बिलियन रुपये या लगभग 29 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाता है। ये जुर्माना तब भी लगाया जा सकता है जब उल्लंघन डीपीआर द्वारा किया गया हो। इसलिए, यह आवश्यक है कि डीएफ अपने डीपीए में "क्षतिपूर्ति खंड" की प्रभावशीलता का मूल्यांकन करे और साथ ही उच्च-स्तरीय परिश्रम करे तथा प्रोसेसर की वरिष्ठ नेतृत्व टीमों से संपर्क करे।

**आगे बढ़ने का मार्ग**

डीएफ को डीपीआर के साथ मौजूदा अनुबंधों की समीक्षा करनी चाहिए ताकि संभावित जोखिमों की पहचान की जा सके, भले ही उन अनुबंधों पर बातचीत संभव न हो। यदि डीएफ के पास डीपीआर के साथ अपने अनुबंध पर बातचीत करने की क्षमता नहीं है, तो उसे यह मूल्यांकन करना चाहिए कि क्या डीपी को असमान सौदेबाजी शक्ति के बारे में सूचित किया जाना चाहिए। डीपीबीआई डीपीडीपीए के कार्यान्वयन के आधार पर, यह खुलासा डीएफ पर जुर्माना लगाने के लिए एक कम करने वाले कारक के रूप में कार्य कर सकता है।

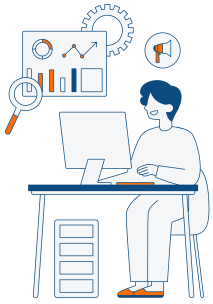
# अवधारणा 5: आयु सीमा का निर्धारण

## 1. कानून क्या दर्शाता है?

डीपीडीपीए की धारा 9 के अनुसार, डीपीडीपी नियमों के नियम 10 के साथ पढ़ते हुए, (i) एक बच्चे (<18 वर्ष की आयु) और (ii) विकलांग व्यक्ति (पीडब्ल्यूडी) जिसके पास वैध अभिभावक हो, की विकलांगता प्रमाण पत्र की प्रक्रिया के लिए सत्यापन योग्य सहमति अनिवार्य है।

**क्यों?**

डीपीडीपीए बच्चों के डेटा की सुरक्षा और जवाबदेही सुनिश्चित करने की आवश्यकता को मान्यता देता है। प्रावधानों में सत्यापन प्रक्रिया को प्रभावी बनाने के लिए पहले से विद्यमान संभावित वर्चुअल टोकन प्रणाली और पहचान उपकरणों का उपयोग करने का प्रयास किया गया है।



## 2. डीएफ को क्या करना चाहिए?

डीएफ को किसी भी बच्चे या पी.डब्ल्यू.डी. डेटा को संसाधित करने से पूर्व माता-पिता/अभिभावक की सत्यापन योग्य सहमति प्राप्त करने के लिए तकनीकी और संगठनात्मक उपायों को लागू करना चाहिए। सहमति को धारा 6 के अंतर्गत सामान्य सहमति प्रावधानों का पालन करना चाहिए और इसके दो अतिरिक्त पहलू हैं:

### माता-पिता की पहचान

माता-पिता/अभिभावक की पहचान और आयु (18 वर्ष से अधिक) की पुष्टि करना। यह सत्यापन के माध्यम से किया जा सकता है।

- आयु और पहचान विवरण पहले से उपलब्ध है, या
- स्वेच्छा से प्रदान की गई सरकार द्वारा जारी पहचान या वर्चुअल टोकन (जैसे डिजिलॉकर)

### संरक्षण का प्रमाण

दिव्यांग व्यक्तियों के लिए, डीएफ को यह सुनिश्चित करना होगा कि अभिभावक की नियुक्ति न्यायालय, नामित प्राधिकारी या स्थानीय स्तर की समिति द्वारा की गई है।

तर्क किया जा सकता है कि डीएफ को यह सत्यापित करने की आवश्यकता नहीं है कि सहमति देने वाला "माता-पिता" बच्चे का वास्तविक माता-पिता है या नहीं।

**क्या सहमति अनिवार्य है?**

हां, किसी बच्चे के पीडी को उपर्युक्त विधियों से सहमति प्राप्त किए बिना संसाधित नहीं किया जा सकता, जब तक कि छूट न दी गई हो।

## 3. छूट

डीपीडीपी नियमों की अनुसूची IV के भाग ए और बी के अंतर्गत कुछ संस्थाओं को विशिष्ट डेटा के लिए सहमति प्राप्त करने से छूट प्रदान की गई है। बच्चों की ट्रैकिंग और व्यवहारिक निगरानी पर लागू प्रतिबंधों के लिए भी छूट मान्य है।

| भाग ए: स्वास्थ्य और शिक्षा | भाग बी: विधि और व्यवस्था |
|---|---|
| स्वास्थ्य देखभाल, मानसिक स्वास्थ्य संस्थानों और संबंधित स्वास्थ्य संस्थानों को बच्चे के स्वास्थ्य की सुरक्षा के लिए आवश्यक सीमा तक डेटा संसाधित करने की अनुमति है।<br><br>क्रेच, चाइल्डकेयर और शैक्षणिक संस्थानों को बच्चे की सुरक्षा के लिए आवश्यक सीमा तक ट्रैकिंग और व्यवहारिक निगरानी डेटा को संसाधित करने की अनुमति है। | कोई भी कानूनी लाभ (सब्सिडी, सेवा, आदि) प्रदान करने और किसी भी कानूनी कर्तव्य के निर्वहन के लिए आवश्यक प्रक्रियाओं को छूट दी गई है।<br><br>उपयोगकर्ता खाता बनाने की प्रक्रिया, यह सुनिश्चित करने के लिए कि हानिकारक जानकारी बच्चों तक न पहुंचे और यह पुष्टि करने के लिए कि डीपी बच्चा नहीं है, भी छूट प्राप्त है। |

**जुर्माना**

हालांकि कोई विशिष्ट दंड निर्धारित नहीं है, लेकिन डीपीडीपीए की अनुसूची *I* के अंतर्गत धारा 33(1) में अधिनियम या संबंधित नियमों के तहत दायित्वों को पूरा करने में विफलता के लिए 2 बिलियन रुपये तक का जुर्माना निर्धारित किया गया है।

## 4. चिंताएँ

| रिक्त स्थान | समस्याएँ |
|---|---|
| • इस विषय पर कोई स्पष्टता नहीं है कि यदि कोई बच्चा झूठा दावा करता है कि वह वयस्क है, तो डीएफ को क्या कार्रवाई करनी चाहिए।<br>• यह सत्यापित करने का कोई उपाय नहीं है कि बच्चे की ओर से सहमति देने वाला व्यक्ति माता-पिता है या नहीं।<br>• यदि बच्चा या दिव्यांग व्यक्ति माता-पिता या कानूनी अभिभावक के बिना है, तो प्रक्रिया में स्पष्टता का अभाव है। | • स्वास्थ्य सेवा और शिक्षा के लिए छूट व्यापक और स्पष्ट हैं।<br>• स्वास्थ्य सेवा को बच्चों के लिए लक्षित विज्ञापनों पर प्रतिबंध से छूट प्रदान की गई है। |

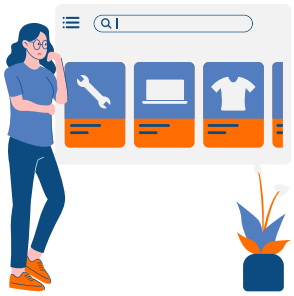
**आगे बढ़ने का मार्ग**

कड़े दंड और स्पष्ट प्रतिबंधों को ध्यान में रखते हुए, डीएफ को यह सुनिश्चित करने के लिए कठोर उपाय अपनाने चाहिए कि माता-पिता की सहमति के बिना किसी भी बच्चे या दिव्यांग व्यक्ति का डेटा संसाधित न किया जाए।

# अवधारणा 6: डेटा संरक्षण

## 1. कानून क्या कहता है?

डीपीडीपीए की धारा 8(7) में उल्लेखित है कि "डीएफ, जब तक किसी कानून के अनुपालन के लिए प्रतिधारण आवश्यक न हो, (क) डीपी द्वारा अपनी सहमति वापस लेने पर या जब यह उचित समझा जाए कि निर्दिष्ट उद्देश्य अब पूरा नहीं हो रहा है, जो भी पहले हो, पीडी को मिटा देगा; और (ख) अपने डीपीआर को किसी भी पीडी को मिटाने के लिए कहेगा जो डीएफ द्वारा ऐसे डीपीआर को प्रसंस्करण के लिए उपलब्ध कराया गया था।"



इन आवश्यकताओं को पूरा करने में किसी भी प्रकार की विफलता पर 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का दंड लगाया जा सकता है।

### निर्धारित लक्ष्य की प्राप्ति

डीपीडीपी नियमों के नियम 8 में तीन प्रकार के डीएफ दिए गए हैं, (ए) भारत में कम से कम 20 मिलियन पंजीकृत उपयोगकर्ताओं वाली ई-कॉमर्स संस्थाएँ, (बी) भारत में कम से कम 20 मिलियन पंजीकृत उपयोगकर्ताओं वाली सोशल मीडिया मध्यस्थ और (सी) भारत में कम से कम 5 मिलियन उपयोगकर्ताओं वाली ऑनलाइन गेमिंग मध्यस्थों को डीपी के व्यक्तिगत डेटा को तीन वर्षों के भीतर मिटाना होगा, जब डीपी ने निर्दिष्ट उद्देश्य की पूर्ति के लिए उनसे संपर्क किया था/अपने अधिकारों का प्रयोग किया था या नियमों के लागू होने से, जो भी पहले हो। इसके अतिरिक्त, डीएफ को डीपी को व्यक्तिगत डेटा हटाने से पहले 48 घंटे का नोटिस देना होगा।

## 2. लागू कानूनों के अनुसार डेटा को कब बनाए रखा जा सकता है?

धारा 38(1) के अनुसार, ये प्रावधान किसी अन्य कानून के अतिरिक्त हैं, न कि उसके उल्लंघन में। धारा 8(7) के साथ पढ़ने पर इसका तात्पर्य यह है कि डीएफ पीडी को तब बनाए रख सकता है, जब किसी अन्य कानून या क्षेत्र-विशिष्ट विनियमों के अनुपालन के लिए ऐसा प्रतिधारण आवश्यक हो। हालाँकि, एकत्र किए गए डेटा की प्रकृति के आधार पर, विशिष्ट प्रतिधारण आवश्यकताएँ विभिन्न क्षेत्रों में भिन्न हो सकती हैं।

### वित्तीय कानूनों के अंतर्गत आवश्यकताएँ

| अधिनियम/विनियमन/नियम | अनुभाग/नियम/पैरा | अवधारणा अवधि | डेटा को संरक्षित करना होगा | आवेदन |
|---|---|---|---|---|
| आयकर अधिनियम, 1961 और आयकर नियम, 1962 | नियम 6(एफ) | 6 साल | हिसाब-किताब | प्रत्येक करदाता |

| अधिनियम/विनियमन/नियम | अनुभाग/नियम/पैरा | अवधारणा अवधि | डेटा को संरक्षित करना होगा | प्रयोज्यता |
|---|---|---|---|---|
| जो वही | नियम 10(डी) | 8 वर्ष | खातों की डायरी | व्यक्ति ने कोई लेनदेन किया, चाहे वह अंतरराष्ट्रीय हो या घरेलू। |
| केंद्रीय वस्तु और सेवा अधिनियम, 2017 | धारा 35 | 6 साल | अभिलेख | कर रिटर्न प्रस्तुत करने वाला कोई भी व्यक्ति |
| कंपनी अधिनियम, 2013 | धारा 128 | 8 वर्ष | हिसाब-किताब | कंपनी |
| धन शोधन निवारण अधिनियम, 2002 | धारा 12 | 5 साल | लेन-देन का अभिलेख और अन्य दस्तावेज़ | रिपोर्टिंग इकाई |
| मुद्रा परिवर्तन गतिविधियों को नियंत्रित करने वाले निर्देशों के ज्ञापन पर मास्टर परिपत्र, 2014 | पैरा 4.13(i) | 5 साल | लेन-देन का अभिलेख | अधिकृत प्रतिनिधि |
| बैंकिंग विनियमन अधिनियम, 1949 बैंकिंग कंपनियों (रिकॉर्ड के संरक्षण की अवधि) नियम, 1985 के साथ | नियम 2 | 5 साल | खाते और अन्य दस्तावेज जैसे चेक बुक रजिस्टर, डिलीवरी ऑर्डर रजिस्टर इत्यादि | बैंकिंग कंपनियाँ |
| जो वही | नियम 3 | 8 वर्ष | खाते और अन्य दस्तावेज जैसे सभी व्यक्तिगत खाता विवरण, अतिदेय ऋण रजिस्टर, आदि | जो वही |

| अधिनियम/विनियमन/नियम | अनुभाग/नियम/पैरा | अवधारणा अवधि | डेटा को संरक्षित करना होगा | प्रयोज्यता |
|---|---|---|---|---|
| भारतीय प्रतिभूति और विनिमय बोर्ड अधिनियम, 2002 प्रतिभूति संविदा (विनियमन) नियम, 1957 के साथ। | नियम 15(1) | 5 साल | लेन-देन का अभिलेख | सेबी द्वारा विनियमित संस्थाएं |
| म्यूचुअल फंड हेतु मास्टर परिपत्र | पैरा 8.5.10 | 8 वर्ष | म्यूचुअल फंड के अभिलेख | मान्यता प्राप्त शेयर बाजार का सदस्य |
| केवाईसी दिशा-निर्देश, पीएमएलए के धन शोधन विरोधी मानक, 2002, एनबीएफसी के दायित्वों पर मास्टर सर्कुलर | पैरा 4 | कम से कम 10 वर्ष | लेन-देन के आवश्यक अभिलेख और अन्य दस्तावेज़ | गैर-बैंकिंग वित्तीय संस्थान |
| केवाईसी दिशा-निर्देश, पीएमएलए के धन शोधन विरोधी मानक, 2002, बैंकों की जिम्मेदारियों पर मास्टर सर्कुलर | पैरा 2.24 (सी) | कम से कम 5 वर्ष | लेन-देन के आवश्यक अभिलेख और अन्य दस्तावेज़ | बैंकों |
| अंतर्राष्ट्रीय वित्तीय सेवा केंद्र प्राधिकरण (भुगतान सेवाएँ) नियम, 2024 | विनियमन 24(4) | 10 वर्ष | लेन-देन का अभिलेख | आईएफएससी में कार्यरत सेवा प्रदाता के लिए भुगतान |
| बीमा अधिनियम, 1938 आर/डब्ल्यू आईआरडीएआई (जांच और निरीक्षण हेतु आवश्यक न्यूनतम जानकारी) विनियम, 2020 | धारा 14(1)(ए) और (बी) विनियमन 24 के साथ | 10 वर्ष | नीति रिकॉर्ड और दावों के दस्तावेज़ | बीमा निगम |
| विदेशी मुद्रा प्रबंधन अधिनियम, 1999 भारत से विभिन्न विप्रेषणों पर मास्टर परिपत्र, 2015 के साथ | पैरा 2.5 | 1 वर्ष | विदेशी मुद्रा बिक्री से संबंधित दस्तावेज़ | अधिकृत प्रतिनिधि |

PSA
LEGAL COUNSELLORS

## प्रौद्योगिकी कानूनों के अंतर्गत आवश्यकताएँ

| अधिनियम/विनियमन/नियम | अनुभाग/नियम/पैरा | अवधारणा अवधि | डेटा को संरक्षित करना होगा | प्रयोज्यता |
|---|---|---|---|---|
| आईटी अधिनियम, 2000 आर/डब्ल्यू सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया नैतिकता) नियम, 2021 | नियम 3(1) (जी) और (एच) | 180 दिन | उपयोगकर्ता पंजीकरण से संबंधित जानकारी और हटाई गई या निष्क्रिय की गई जानकारी | मध्यस्थ |
| आधार (वित्तीय और अन्य सब्सिडी, लाभ और सेवाओं का लक्षित वितरण) अधिनियम, 2016 आर/डब्ल्यू आधार प्रमाणीकरण विनियम, 2016 | नियम 26 और 27 | 6 महीने और 5 वर्षों के लिए संग्रहीत | प्रमाणन अभिलेख | भारतीय विशिष्ट पहचान प्राधिकरण |
| आधार (वित्तीय और अन्य सब्सिडी, लाभ और सेवाओं का लक्षित वितरण) अधिनियम 2016 आर/डब्ल्यू आधार प्रमाणीकरण और ऑफ़लाइन सत्यापन विनियमन, 2021 | नियम 18(1) से (3) और 20(1) से (3) | 2 वर्ष और 5 वर्ष से संग्रहीत | प्रमाणीकरण लेनदेन का लॉग | अनुरोधकर्ता संगठन और प्रमाणीकरण सेवा एजेंसियां |
| दूरसंचार अधिनियम, 2023 दूरसंचार विभाग के 21 अक्टूबर, 2021 के परिपत्र के साथ (एकीकृत लाइसेंस समझौते में संशोधन) | पैरा 1 | 2 साल | वाणिज्यिक अभिलेख, कॉल विवरण, विनिमय विवरण अभिलेख, आईपी विवरण अभिलेख | एकीकृत लाइसेंस धारक |
| CERT-In दिशा-निर्देश, 2022 | पैरा (iv) | 180 दिन | सूचना संचार प्रौद्योगिकी प्रणाली के लॉग | सेवा प्रदाता, मध्यस्थ, डेटा केंद्र और एक कॉर्पोरेट संस्था |

| अधिनियम/विनियमन/नियम | अनुभाग/नियम/पैरा | अवधारणा अवधि | डेटा को संरक्षित करना होगा | प्रयोज्यता |
|---|---|---|---|---|
| *CERT-In* दिशा-निर्देश, 2022 | पैरा (iv) | 5 साल | केवाईसी विवरण और वित्तीय लेनदेन के अभिलेख | वर्चुअल संपत्ति सेवा प्रदाता, वर्चुअल संपत्ति विनिमय प्रदाता और कस्टोडियन वॉलेट प्रदाता |

## स्वास्थ्य कानूनों के अंतर्गत आवश्यकताएँ

| अधिनियम/विनियमन/नियम | अनुभाग/नियम/पैरा | अवधारणा अवधि | डेटा को संरक्षित करना होगा | प्रयोज्यता |
|---|---|---|---|---|
| भारतीय आयुर्विज्ञान परिषद अधिनियम, 1956 और चिकित्सा आचार संहिता विनियम, 2002 | विनियमन 1.3.1 | 3 वर्ष | इनडोर रोगियों के चिकित्सा अभिलेख | प्रत्येक चिकित्सकगण |
| इलेक्ट्रॉनिक स्वास्थ्य रिकॉर्ड मानक, 2016 | पैराऐलेक्ट्रॉनिक चिकित्सा रिकॉर्ड संरक्षण, पृष्ठ 22 | रोगी का जीवनकाल | इलेक्ट्रॉनिक चिकित्सा रिकॉर्ड | चिकित्सक या स्वास्थ्य सेवा संस्थान |
| नैदानिक प्रतिष्ठान (पंजीकरण और विनियमन) अधिनियम, 2010, नैदानिक प्रतिष्ठान (केंद्र सरकार) नियम, 2012 के साथ। | नियम 9(iv) | राज्य के अनुसार भिन्नता होती है। | इलेक्ट्रॉनिक चिकित्सा/स्वास्थ्य अभिलेख | प्रत्येक चिकित्सीय प्रतिष्ठान |

PSA LEGAL COUNSELLORS

## अन्य कानूनों के तहत आवश्यकताएँ

| अधिनियम/विनियमन/नियम | अनुभाग/नियम/पैरा | अवधारणा अवधि | डेटा को संरक्षित करना होगा | प्रयोज्यता |
|---|---|---|---|---|
| सार्वजनिक अभिलेख अधिनियम, 1993 और अभिलेख प्रतिधारण अनुसूची, 2012 | भौतिक रिकॉर्ड श्रेणी सी, पृष्ठ सप्तम् | श्रेणी के अनुसार 3, 5, 10 वर्ष | सार्वजनिक दस्तावेज | सरकारी संस्थाएँ और सार्वजनिक प्राधिकरण |
| सूचना का अधिकार अधिनियम, 2005 | धारा 8(3) | 20 वर्ष | विभाग द्वारा संधारित सार्वजनिक अभिलेख | सरकारी संस्थाएँ और सार्वजनिक प्राधिकरण |
| नागरिक उड्डयन मंत्रालय के प्रमुख कार्यों से संबंधित अभिलेखों के लिए प्रतिधारण अनुसूची | पैरा (xvi) और (xvii) | श्रेणी के अनुसार 3, 5, 10, 25 वर्ष | सार्वजनिक दस्तावेज | नागरिक उड्डयन मंत्रालय के विभिन्न विभागों |
| न्यूनतम मजदूरी अधिनियम, 1948 न्यूनतम मजदूरी केंद्रीय नियम, 1950 के साथ | नियम 26ए | 3 वर्ष | कर्मचारी जानकारी और अन्य | प्रत्येक नियोक्ता |
| मजदूरी भुगतान अधिनियम, 1936 | धारा 13ए | 3 वर्ष | वेतन अभिलेख | प्रत्येक नियोक्ता |

### आगे बढ़ने का मार्ग

डीपीडीपी नियमों की वर्तमान संरचना के अनुसार, ऐसा प्रतीत होता है कि नियम 8 के अंतर्गत आने वाले डीएफ के अलावा अन्य डीएफ भी अपनी डेटा प्रतिधारण अवधि निर्धारित कर सकते हैं। इससे डीएफ को पर्याप्त लचीलापन प्राप्त होगा, बशर्ते कि उनकी निर्धारित अवधारण अवधि अत्यधिक या अनुचित न हो। हम अनुशंसा करते हैं कि डीएफ एक डेटा प्रतिधारण नीति तैयार करें, जहाँ वे सीमा अधिनियम, 1963 के तहत सामान्य आवश्यकता का अनुपालन करने के लिए कम से कम 3 वर्षों की अवधि के लिए डेटा को बनाए रख सकें। निश्चित रूप से, इसे किसी अन्य क्षेत्रीय कानून के अधीन भी होना चाहिए।

अंत में, डेटा प्रतिधारण दायित्वों को भी डीएफ के साथ निष्पादित डीपीए के माध्यम से डीपीआर को सौंपा जाना चाहिए।

जीडीपीआर के अध्याय 3 के अंतर्गत, डीसी को डीएस के अधिकारों का संरक्षण सुनिश्चित करने के लिए बाध्य किया गया है, यह सुनिश्चित करते हुए कि सभी आवश्यक संचार और कार्य अनुरोध प्राप्त होने के 1 महीने के भीतर बिना किसी देरी के पूरे किए जाएं (जो 3 महीने तक बढ़ाए जा सकते हैं)। इसके अतिरिक्त, यदि कोई अनुरोध पूरा नहीं किया जा सकता है, तो डीएस को 1 महीने के भीतर कारणों के बारे में सूचित किया जाना चाहिए।

सभी संचार संक्षिप्त, पारदर्शी, समझने योग्य और आसानी से सुलभ प्रारूप में, स्पष्ट और सरल भाषा का उपयोग करते हुए प्रस्तुत किए जाने चाहिए। सभी अनुरोधों को निःशुल्क पूरा किया जाना चाहिए, जब तक कि अनुरोध दोहराए न जाएं; ऐसी स्थिति में उचित शुल्क लिया जा सकता है या अनुरोध को अस्वीकार किया जा सकता है।

डीपीडीपीए, आर/डब्ल्यू डीपीडीपी नियमों के अनुसार, डीएफ को डीपी को कुछ अधिकार प्रदान करने की आवश्यकता है। उदाहरण के लिए, पहुँच का अधिकार, शिकायत निवारण, आदि। इसके अतिरिक्त, अनुरोध करने के साधन या शिकायत निवारण की समयसीमा को डीएफ/सहमति प्रबंधक की वेबसाइट या ऐप पर सूचीबद्ध किया जाना चाहिए (नियम 13)। डीएफ को कोई शुल्क लेने का अधिकार नहीं दिया गया है।

## सहमति एवं वापसी

### जीडीपीआर

जहां व्यक्तिगत डेटा (पीडी) को सीधे डेटा स्रोत (डीएस) से एकत्र किया जाता है, वहां डीसी को उसकी पहचान और उसके/डीपीओ के संपर्क विवरण, संग्रह का उद्देश्य, कानूनी आधार, वैध हित, डेटा प्राप्तकर्ता, सीमा पार स्थानांतरण, अवधारण अवधि, डेटा विषय के अधिकार (वापसी, मिटाना, शिकायत दर्ज करना आदि), डेटा न देने के परिणाम और स्वचालित निर्णय लेने से संबंधित जानकारी प्रदान करनी चाहिए। अप्रत्यक्ष संग्रह के लिए, डीसी को एकत्रित पीडी का स्रोत और श्रेणियां भी प्रदान करनी चाहिए (अनुच्छेद 13 और 14)।

इसके अतिरिक्त, डीएस किसी भी समय अपनी सहमति वापस ले सकते हैं (अनुच्छेद 7(3))।

### डीपीडीपीए

डीपी से सहमति प्राप्त करने के लिए एक नोटिस संलग्न किया जाना चाहिए, जिसमें एकत्रित की जाने वाली पीडी, इच्छित उद्देश्य, वह प्रक्रिया जिसके माध्यम से डीपी सहमति वापस ले सकता है या शिकायत निवारण तक पहुंच सकता है, और डीपीबीआई को शिकायत करने की प्रक्रिया का उल्लेख हो (धारा 5)।

इसके अतिरिक्त, डीपी किसी भी समय अपनी सहमति वापस ले सकता है (धारा 6(4))।

PSA LEGAL COUNSELLORS

### तुलना

जीडीपीआर के अंतर्गत, डेटा संग्रह के समय प्रदान की जाने वाली जानकारी विस्तृत और समग्र होती है। इसके विपरीत, डीपीडीपीए अपने सहमति नोटिस में केवल सीमित खुलासे को अनिवार्य करता है। यदि जीडीपीआर का अनुपालन करने वाली कोई कंपनी सहमति के आधार पर पीडी की प्रक्रिया करती है, तो वह डीपीडीपीए के तहत सहमति आवश्यकताओं का पालन भी करेगी। बेशक, यह एक चेतावनी के साथ है कि जीडीपीआर अन्य आधारों पर भी पीडी की प्रक्रिया की अनुमति देता है।

## पहुँच की जानकारी

### जीडीपीआर

डीएस डीसी से यह पुष्टि करने के लिए पूछ सकता है कि क्या उसके पीडी पर कार्रवाई की जा रही है। यदि हां, तो वह संग्रह के उद्देश्य, एकत्रित पीडी की श्रेणियां, प्राप्तकर्ताओं का विवरण (सीमा पार सहित), अवधारण अवधि, अन्य अधिकारों की जानकारी, संग्रह स्रोत (यदि डीएस से एकत्र नहीं किया गया है), और किसी भी स्वचालित निर्णय लेने की मौजूदगी (अनुच्छेद 15) के बारे में पूछ सकता है।

### डीपीडीपीए

डीपी, कुछ प्रतिबंधों के अधीन, अपने संसाधित पीडी का सारांश, की गई प्रसंस्करण गतिविधियां, डीएफ और डीपीआर की पहचान जिनके साथ डेटा साझा किया गया है, आदि तक पहुंच प्राप्त कर सकते हैं (धारा 11)।

### तुलना

जीडीपीआर में एक्सेस के अधिकारों का विस्तृत विवरण प्रस्तुत किया गया है। जीडीपीआर का अनुपालन करने वाले डेटा फ़िड्युसरी द्वारा डीपीडीपीए के अंतर्गत डेटा प्रिंसिपल अधिकारों का पालन किए जाने की संभावना अत्यधिक है।

## सुधार और विलोपन

### जीडीपीआर

डीएस गलत या अधूरे पीडी और विलोपन में सुधार या पूर्णता का अनुरोध कर सकता है, जहां उद्देश्य पूरा हो गया है, प्रसंस्करण अवैध है, नहीं

### डीपीडीपीए

डीपी में गलतियों या अधूरे पीडी के सुधार, पूर्णता या अद्यतन के लिए अनुरोध किया जा सकता है। इसके अतिरिक्त, वे हटाने का भी अनुरोध कर सकते हैं।

गैरकानूनी, कोई कानूनी या वैध आधार मौजूद नहीं है, कानून द्वारा मिटाने की आवश्यकता है, या पीडी को समाज सेवाओं के लिए एकत्र किया गया था। हालाँकि, डीसी अभिव्यक्ति की स्वतंत्रता, कानूनी दायित्वों, सार्वजनिक स्वास्थ्य में सार्वजनिक हित, कानूनी दावों, या सार्वजनिक हित में संग्रह उद्देश्यों, वैज्ञानिक या ऐतिहासिक अनुसंधान/सांख्यिकीय उद्देश्यों (अनुच्छेद 16 और 17) के अपने अधिकार के प्रयोग के लिए आवश्यक होने पर पीडी को बनाए रख सकता है।

पीडी का विलोपन। हालाँकि, डीएफ निर्दिष्ट उद्देश्य की पूर्ति/या कानून के अनुपालन के लिए पीडी की प्रक्रिया जारी रख सकता है (धारा 12)।

### तुलना

जीडीपीआर के तहत मिटाने का अधिकार सीमित है, क्योंकि इसमें उन आधारों की सूची दी गई है जिन पर मिटाने का अनुरोध किया जा सकता है। यह उन अपवादों को भी स्पष्ट करता है जहाँ मिटाने से इनकार किया जा सकता है, जैसे कि अभिव्यक्ति की स्वतंत्रता, कानूनी दायित्व या सार्वजनिक हित। इसके विपरीत, डीपीडीपीए डीपी को किसी भी कारण से मिटाने का अनुरोध करने की अनुमति देता है, केवल उद्देश्य की पूर्ति या कानून के अनुपालन के लिए निरंतर प्रसंस्करण के साथ। जीडीपीआर का अनुपालन करने वाले डीएफ को डीपीडीपीए के अनुपालन के लिए इस अधिकार पर पुनर्विचार करना होगा।

## शिकायत समाधान

### जीडीपीआर

डीएस अपने निवास, कार्यस्थल या जहां कथित उल्लंघन हुआ है, वहां के सदस्य राज्य में पर्यवेक्षी प्राधिकरण से शिकायत कर सकते हैं। डी.एस. अन्य प्रशासनिक या न्यायिक उपायों का भी सहारा ले सकते हैं (अनुच्छेद 77)।

### डीपीडीपीए

डीपी को अपनी किसी भी शिकायत के लिए सबसे पहले डीएफ या सहमति प्रबंधक (यदि लागू हो) से संपर्क करना आवश्यक है। डीपीबीआई (धारा 13) से संपर्क करने से पूर्व यह उपाय समाप्त होना चाहिए।

### तुलना

जीडीपीआर में डीसी को शिकायत निवारण तंत्र प्रदान करने की स्पष्ट आवश्यकता नहीं है। इसके बजाय, विवाद की स्थिति में डेटा सब्जेक्ट सीधे पर्यवेक्षी प्राधिकरण के पास शिकायत दर्ज कर सकता है। इसके विपरीत, डीपीडीपीए डीएफ को डेटा प्रोसेसर द्वारा डेटा प्रोसेसिंग बुनियादी ढांचे से संपर्क करने से पहले चिंताओं का निवारण करने का निर्देश देता है। जीडीआर के अनुरूप डीएफ को यह सुनिश्चित करना होगा कि उनके पास डेटा प्रोसेसर द्वारा उठाई गई शिकायतों को संबोधित करने के लिए आवश्यक साधन और बैंडविड्थ उपलब्ध है।

PSA
LEGAL COUNSELLORS

## अन्य अधिकार

### जीडीपीआर

- **प्रसंस्करण पर प्रतिबंध:** यदि (क) पीडी गलत है, (ख) पीडी अवैध रूप से संसाधित किया गया है, (ग) पीडी को अब डीसी द्वारा संसाधित करने की आवश्यकता नहीं है, लेकिन डीएस को कानूनी दावों की स्थापना, प्रयोग या बचाव के लिए डीसी द्वारा इसे संसाधित करने की आवश्यकता है, या (घ) इसने आपत्ति करने के अपने अधिकार का प्रयोग किया है (अनुच्छेद 18)।

- **अधिसूचना दायित्व:** डीसी को सभी डेटा प्राप्तकर्ताओं को डीएस द्वारा किए गए सभी सुधार, विलोपन या प्रसंस्करण प्रतिबंध अनुरोधों के संबंध में सूचित करना आवश्यक है (अनुच्छेद 19)।

- **डेटा पोर्टेबिलिटी का अधिकार:** डीएस डीसी से अनुरोध कर सकता है कि वे अपने पीडी को संरचित, मशीन-पठनीय प्रारूप में साझा करें। इसके पश्चात, डीएस इस डेटा को किसी अन्य डीसी को स्थानांतरित कर सकता है, बशर्ते मूल प्रसंस्करण सहमति या अनुबंध पर आधारित हो और स्वचालित साधनों का उपयोग करके किया गया हो (अनुच्छेद 20)।

- **आपत्ति का अधिकार:** डीएस प्रोफाइलिंग सहित किसी भी प्रसंस्करण पर आपत्ति की जा सकती है, और डीसी को ऐसी प्रसंस्करण को जारी रखने के लिए वैध आधार प्रस्तुत करना होगा (अनुच्छेद 21(1))।

- **स्वचालित निर्णय लेना:** डीएस केवल स्वचालित प्रसंस्करण द्वारा लिए गए निर्णयों के अधीन नहीं हो सकता है, जिसमें प्रोफाइलिंग भी शामिल है, जो कानूनी प्रभाव उत्पन्न करता है, सिवाय उन मामलों के जहां निर्णय किसी अनुबंध के लिए आवश्यक हैं, कानून द्वारा अधिकृत हैं, या स्पष्ट डीएस सहमति (अनुच्छेद 22) पर आधारित हैं।

### डीपीडीपीए

- **नामांकन का अधिकार:** डीपी अपनी मृत्यु या अक्षमता की स्थिति में अपने अधिकारों का प्रयोग करने के लिए किसी अन्य व्यक्ति को नामित कर सकते हैं (धारा 14)।

### निष्कर्ष

एक मिथक है कि जीडीपीआर का अनुपालन डीपीडीपीए का अनुपालन करने के लिए पर्याप्त है। लेकिन, विषय की गहरायी में जाना ज़रूरी है। हालाँकि जीडीपीआर डेटा विषयों को अधिक अधिकार प्रदान करता है, लेकिन इसके साथ कुछ शर्तें भी जुड़ी हुई हैं। उदाहरण के लिए, मिटाने का अधिकार एक अप्रतिबंधित अधिकार है, लेकिन इसका प्रयोग केवल तभी किया जा सकता है जब अनुच्छेद 17(1) में उल्लिखित कुछ शर्तें पूरी हों। हालाँकि, डीपीडीपीए के तहत, यह एक पूर्ण अधिकार है, एकमात्र अपवाद यह है कि डीएफ को निर्दिष्ट उद्देश्य को पूरा करने या कानून का पालन करने के लिए व्यक्तिगत डेटा को संसाधित करना आवश्यक है। इसलिए, यदि आप जीडीपीआर का अनुपालन करते हैं, तो आपको अभी भी डीपीडीपीए के अनुपालन को सुनिश्चित करने के लिए कदम उठाने होंगे। डेटा विषयों को दिए गए अधिकारों का अनुपालन न करने पर 500 मिलियन रुपये या लगभग अमेरिकी डॉलर 6 मिलियन प्रति उल्लंघन तक का जुर्माना लग सकता है।

## क्या होगा यदि "डेटा विषय अधिकार" पर ये जीडीपीआर मामले भारत में घटित हों?

### डेटा विषय अधिकार क्या होते हैं?

जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर) के अध्याय 3 के अंतर्गत, डीसी को डीएस को विभिन्न अधिकार प्रदान करने के लिए बाध्य किया जाता है, जैसे कि सूचित किए जाने का अधिकार (अनुच्छेद 13 और 14), पहुंच का अधिकार (अनुच्छेद 15), सुधार का अधिकार (अनुच्छेद 16), मिटाने का अधिकार (अनुच्छेद 17), प्रसंस्करण को प्रतिबंधित करने का अधिकार (अनुच्छेद 18), आपत्ति करने का अधिकार (अनुच्छेद 21) आदि, जिन्हें सामूहिक रूप से डीएस अधिकार कहा जाता है।

**डीपी अधिकार क्या होते हैं?**

डीपीडीपीए में डीएफ से यह भी अपेक्षा की गई है कि वे डीपी को कुछ अधिकार प्रदान करें, जिनमें पहुंच का अधिकार (धारा 11), सुधार और विलोपन का अधिकार (धारा 12), शिकायत निवारण का अधिकार (धारा 13) और नामांकन का अधिकार (धारा 14) शामिल हैं, जिन्हें सामूहिक रूप से डीपी अधिकार के रूप में जाना जाता है।

### मुख्य निर्णय

#### 1. ऑस्ट्रिया - मिटाने का अधिकार

- **पृष्ठभूमि:** ऑस्ट्रिया में स्थित एक संस्था जिसने फुटबॉल लीग का आयोजन किया, ने अपनी वेबसाइट पर उन खिलाड़ियों की जानकारी प्रकाशित की जिन्होंने लीग मैचों में भाग लिया। इस जानकारी में नाम, फोटो, राष्ट्रीयता आदि जैसे व्यक्तिगत डेटा शामिल थे। 23 सितंबर, 2020 को, श्री रॉबर्टो, एक फुटबॉल खिलाड़ी जिन्होंने पहले मैचों में भाग लिया, ने वेबसाइट से अपने व्यक्तिगत डेटा को हटाने का अनुरोध करते हुए एक ई-मेल भेजा। लेकिन, संस्था ने सांख्यिकीय उद्देश्यों के लिए व्यक्तिगत डेटा को बनाए रखने की आवश्यकता का हवाला देते हुए इनकार कर दिया। परिणामस्वरूप, श्री रॉबर्टो ने Österreichische Datenschutzbehörde, यानी ऑस्ट्रियाई डेटा संरक्षण प्राधिकरण (**ऑस्ट्रियाई डीपीए**) के साथ शिकायत दर्ज की।

- **निष्कर्ष:** ऑस्ट्रियाई डीपीए ने जीडीपीआर के अनुच्छेद 17(1) का उल्लेख किया, जो डीएस को बिना किसी देरी के अपने व्यक्तिगत डेटा को मिटाने का अनुरोध करने का अधिकार प्रदान करता है। यदि अनुच्छेद 17(1)(ए) से (एफ) के तहत कोई भी शर्त पूरी होती है, तो नियंत्रकों के लिए इसका पालन करना अनिवार्य है। वर्तमान मामले में, श्री रॉबर्टो ने फिर कभी भाग न लेने के इरादे से अपने व्यक्तिगत डेटा को हटाने का अनुरोध किया था। इसलिए, अनुच्छेद 17(1)(ए) के अनुसार, व्यक्तिगत डेटा "उन उद्देश्यों के संबंध में अब आवश्यक नहीं था जिनके लिए उन्हें एकत्र किया गया था या अन्यथा संसाधित किया गया था"। नतीजतन, **4 जनवरी, 2024** को गैर-अनुपालन के लिए 11,000 यूरो या लगभग 12,500 अमेरिकी डॉलर का जुर्माना, साथ ही लागत के लिए 1,100 यूरो या लगभग 1,250 अमेरिकी डॉलर का जुर्माना लगाया गया।

**भारत में क्या होगा?**

- **प्रासंगिक डीपीडीपीए प्रावधान:** डीपीडीपीए की धारा 12(3) के अनुसार, डीएफ, मिटाने के अनुरोध के प्राप्त होने पर, पीडी को मिटा देगा, जब तक कि निर्दिष्ट उद्देश्य की पूर्ति या लागू कानून के अनुपालन के लिए अवधारण आवश्यक न हो।

- **जुर्माना:** उपरोक्त मामले के तथ्यों के अनुसार, डेटा मिटाने के अनुरोधों का अनुपालन न करने पर प्रत्येक उल्लंघन के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है।

## 2. स्पेन - पहुंच का अधिकार

- **पृष्ठभूमि:** माइकल पेज इंटरनेशनल, यूनाइटेड किंगडम में स्थित एक रोजगार एजेंसी है, जिसकी यूरोप भर में सहायक कंपनियाँ हैं, जो "माइकल पेज" सहित विभिन्न ब्रांडों के तहत संचालित होती हैं। शिकायतकर्ता, एक डच नागरिक, ने माइकल पेज की वेबसाइट पर एक खाता बनाया और अपना बायोडाटा अपलोड किया। 28 सितंबर, 2018 को, उसने अपने व्यक्तिगत डेटा तक पहुँचने के लिए एक अनुरोध भेजा। हालाँकि, कंपनी ने उसकी पहचान सत्यापित करने के लिए एक आईडी माँगते हुए उसके अनुरोध को रोक दिया। इस प्रकार, शिकायतकर्ता ने डच डेटा सुरक्षा प्राधिकरण के समक्ष एक शिकायत दर्ज की, जिसमें कहा गया कि डेटा एक्सेस अनुरोध को पूरा करने के लिए आईडी माँगना अत्यधिक था। बाद में, मामला एजेंसिया एस्पानोला डे प्रोटेक्शन डे डेटास यानी स्पेनिश डेटा सुरक्षा प्राधिकरण (**स्पेनिश डीपीए**) को स्थानांतरित कर दिया गया।

- **निष्कर्ष:** स्पेनिश डीपीए ने यह निर्धारित किया कि पहचान सत्यापन प्रक्रिया केवल तभी लागू होनी चाहिए जब अनुरोध करने वाले व्यक्ति की पहचान के संबंध में उचित संदेह उत्पन्न हो। वर्तमान मामले में, नियंत्रक उचित संदेह के अस्तित्व को प्रमाणित करने में असफल रहा। इसके बजाय, पहचान सत्यापन एक मानक प्रक्रिया के रूप में कार्य कर रहा था। इसलिए, नियंत्रक को अनुच्छेद 12(2) और 12(3) का उल्लंघन करने का दोषी ठहराया गया। परिणामस्वरूप, **25 फरवरी, 2022** को प्रकाशित एक निर्णय के माध्यम से 300,000 यूरो या लगभग 334,000 अमेरिकी डॉलर का जुर्माना लगाया गया।

**भारत में क्या होगा?**

- **प्रासंगिक डीपीडीपीए प्रावधान:** डीपीडीपीए की धारा 11 के अंतर्गत, डीपी डीएफ से अपने पीडी तक पहुंच का अनुरोध कर सकता है। ऐसा अनुरोध प्राप्त होने पर, डीएफ को संसाधित किए जा रहे पीडी और किए गए प्रसंस्करण गतिविधियों का सारांश प्रदान करना अनिवार्य है। इसके अतिरिक्त, कुछ शर्तों के अधीन, डीएफ को प्रदान करनी होगी (i) डीएफ और डीपीआर की पहचान जिनके साथ डेटा साझा किया गया है, साथ ही साझा किए गए डेटा का विवरण; और (ii) कोई अन्य प्रासंगिक जानकारी।

- **जुर्माना:** उपरोक्त मामले के तथ्यों को ध्यान में रखते हुए, डेटा एक्सेस अनुरोधों को पूरा करने में विफलता के कारण प्रत्येक उल्लंघन पर 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है।

### 3. चेक गणराज्य - सूचना का अधिकार

- **पृष्ठभूमि:** चेक गणराज्य में स्थित कंपनी डीसी पर आरोप है कि उसने अपने एंटीवायरस सॉफ़्टवेयर के उपयोगकर्ताओं के व्यक्तिगत डेटा को अपनी सहयोगी कंपनी को हस्तांतरित कर दिया। यह हस्तांतरण उपयोगकर्ता की सहमति के बिना किया गया। इसके अतिरिक्त, नियंत्रक ने उपयोगकर्ताओं को इस संबंध में भ्रामक जानकारी प्रदान की, यह दावा करते हुए कि हस्तांतरित डेटा को गुमनाम किया गया था और इसका उपयोग केवल सांख्यिकीय प्रवृत्ति विश्लेषण के लिए किया गया था। इसके परिणामस्वरूप, Úřad pro ochranu osobních údajů यानी चेक डेटा प्रोटेक्शन अथॉरिटी (**चेक डीपीए**) के साथ-साथ कई मीडिया रिपोर्टों के माध्यम से एक गुमनाम शिकायत दर्ज की गई।

- **निष्कर्ष:** जांच के उपरांत, चेक डीपीए ने निष्कर्ष निकाला कि नियंत्रक ने अपने एंटीवायरस सॉफ़्टवेयर और ब्राउज़र एक्सटेंशन के उपयोगकर्ताओं के व्यक्तिगत डेटा को अपनी सहयोगी कंपनी को अवैध रूप से स्थानांतरित कर दिया था, जिससे लगभग 100 मिलियन उपयोगकर्ता प्रभावित हुए। डेटा में अद्वितीय पहचानकर्ताओं से जुड़े छद्म नाम वाले ब्राउज़िंग इतिहास शामिल थे। इसके अतिरिक्त, चेक डीपीए ने यह भी निर्धारित किया कि पुनः पहचान के जोखिम के कारण आंशिक ब्राउज़िंग इतिहास भी व्यक्तिगत डेटा का गठन कर सकता है। परिणामस्वरूप, नियंत्रक के कृत्यों को अनुच्छेद 6 (ए) और 13 (1) का उल्लंघन माना गया, और **10 अप्रैल, 2024** को 13.9 मिलियन यूरो या लगभग 15.8 मिलियन अमेरिकी डॉलर का जुर्माना लगाया गया।

### भारत में क्या होगा?

- **प्रासंगिक डीपीडीपीए प्रावधान:** डीपीडीपीए की धारा 5(1)(i) और धारा 5(2)(i) के अनुसार, डीएफ को डेटा विषय को "व्यक्तिगत डेटा और जिस उद्देश्य के लिए इसे संसाधित किया गया है" के बारे में जानकारी प्रदान करने की आवश्यकता होती है। इसके अतिरिक्त, धारा 6(1) के अनुसार प्राप्त सहमति उस उद्देश्य तक सीमित होनी चाहिए जिसके लिए इसे प्राप्त किया गया था।

- **जुर्माना:** उपरोक्त मामले के तथ्यों को ध्यान में रखते हुए, निर्दिष्ट उद्देश्य से परे पीडी के उपयोग पर प्रति उल्लंघन 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है।

जीडीपीआर के अंतर्गत, डेटा विषय को सूचित किए जाने का अधिकार है जब (*i*) जानकारी सीधे उनसे एकत्र की जाती है (अनुच्छेद 13) या (*ii*) जानकारी अन्य स्रोतों से प्राप्त की जाती है (अनुच्छेद 14)। जबकि डीपीडीपीए के तहत डीएफ (मान लें कि डीएफ 2) को विशेष रूप से यह खुलासा करने की आवश्यकता नहीं है कि क्या उसे किसी अन्य फिड्यूशियरी (मान लें कि डीएफ 1 जिसने मूल रूप से फिड्यूशियरी 2 के साथ डेटा साझा करने के लिए सहमति प्राप्त की थी) से व्यक्तिगत डेटा प्राप्त हुआ है, हम अनुशंसा करते हैं कि जब भी कोई डेटा विषय अपने एक्सेस के अधिकार का प्रयोग करता है, तो इसका खुलासा किया जाना चाहिए।

### 4. इटली - सुधार और विलोपन का अधिकार

- **पृष्ठभूमि:** डीसी इटली में स्थित एक चिकित्सा केंद्र है। डेटा विषय ने अपने COVID-19 PCR परीक्षण के परिणामों तक पहुँच का अनुरोध किया, लेकिन उन्हें गलत ईमेल पते पर भेजा गया। इसके अतिरिक्त, परिणाम प्राप्त करने के बाद, उन्होंने देखा कि रिपोर्ट में जन्म तिथि और कर आईडी जैसी कुछ त्रुटियाँ थीं। इसके बाद, उन्होंने डीसी से अपने व्यक्तिगत डेटा को सुधारने (अनुच्छेद 16) और मिटाने (अनुच्छेद 17) तथा प्रसंस्करण को प्रतिबंधित करने (अनुच्छेद 18) का अनुरोध किया। हालाँकि, उन्हें कोई प्रतिक्रिया नहीं मिली। इस प्रकार, उन्होंने Garante per la protezione dei dati personali, यानी इतालवी डेटा सुरक्षा प्राधिकरण (**इटैलियन डीपीए**) के समक्ष शिकायत दर्ज की।

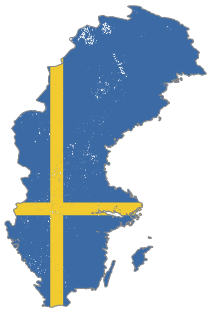
- **निष्कर्ष:** इतालवी डीपीए ने यह निष्कर्ष निकाला कि डेटा की सटीकता सुनिश्चित करना डीसी की जिम्मेदारी थी, जिसे अद्यतित रखने में वह विफल रहा। इसके अतिरिक्त, रिपोर्ट एक अनधिकृत तीसरे पक्ष को भेजी गई, जो नियंत्रक के सुरक्षा दायित्व का उल्लंघन था। इसके अलावा, नियंत्रक एक महीने के भीतर अनुरोध का उत्तर देने में असफल रहा। परिणामस्वरूप, **31 अगस्त, 2023** को अनुच्छेद 12, 15, 16, 17 और 18 के उल्लंघन के लिए 10,000 यूरो या लगभग 11,500 अमरीकी डॉलर का जुर्माना लगाया गया।

### भारत में क्या होगा?

- **प्रासंगिक डीपीडीपीए प्रावधान:** डीपीडीपीए की धारा 12 के अनुसार, डीपी को अपने पीडी में सुधार, पूर्णता या अद्यतन का अनुरोध करने का अधिकार है। ऐसा अनुरोध प्राप्त होने पर, डीएफ को गलत, भ्रामक या अधूरे पीडी को सही, पूर्ण और अद्यतन करना चाहिए। इसके अतिरिक्त, मिटाने के अनुरोध पर, डीएफ को पीडी को मिटा देना चाहिए, जब तक कि निर्दिष्ट उद्देश्य की पूर्ति के लिए या लागू कानून के तहत प्रतिधारण की आवश्यकता न हो।

- **जुर्माना:** उपरोक्त मामले के तथ्यों को ध्यान में रखते हुए, डेटा सुधार और मिटाने के अनुरोधों का अनुपालन न करने पर प्रत्येक उल्लंघन के लिए 500 मिलियन रुपये या लगभग 6 मिलियन अमरीकी डॉलर तक का जुर्माना और 1 बिलियन रुपये या लगभग 12 मिलियन अमरीकी डॉलर तक का कुल जुर्माना लगाया जा सकता है।

### 5. स्वीडन - पहुंच का अधिकार



- **पृष्ठभूमि:** Spotify AB, एक डिजिटल संगीत, पॉडकास्ट और वीडियो स्ट्रीमिंग सेवा, जिसकी स्थापना 2006 में हुई और जिसका मुख्यालय स्वीडन में स्थित है, जनवरी 2019 में Integritetsskyddsmyndigheten, अर्थात् स्वीडिश डेटा प्रोटेक्शन अथॉरिटी (**स्वीडिश डीपीए**) द्वारा एक औपचारिक जांच का विषय बनी। इसके पश्चात "noyb" की शिकायत के साथ-साथ नीदरलैंड और डेनमार्क से अतिरिक्त शिकायतें भी प्राप्त हुईं, जिसमें आरोप लगाया गया कि Spotify ने डेटा एक्सेस अनुरोधों के उत्तर में अधूरी और अस्पष्ट जानकारी प्रदान की। जांच का उद्देश्य यह मूल्यांकन करना था कि Spotify AB की सामान्य प्रथाएँ एक्सेस अनुरोधों को संभालने में जीडीपीआर के अनुपालन में हैं या नहीं।

- **निष्कर्ष:** स्वीडिश डीपीए ने निष्कर्ष निकाला कि पीडी तक पहुँच प्रदान करने की स्पॉटिफ़ाई की विधि अनुच्छेद 15 की सामान्य आवश्यकताओं को पूरा करती है, लेकिन जानकारी को इस प्रकार प्रस्तुत नहीं किया गया कि वह पहुँच के अधिकार के उद्देश्य को पूरा करे। विशेष रूप से, इसने डीएस को यह समझने में असमर्थ रखा कि उनके डेटा को कैसे संसाधित किया जा रहा था या वैध आधार का आकलन कैसे किया जा रहा था। इसके अतिरिक्त, प्रदान की गई जानकारी संक्षिप्त, स्पष्ट या आसानी से सुलभ नहीं थी, जो अनुच्छेद 12(1), 15(1)(ए) से (डी), (जी) और 15(2) का उल्लंघन करती है। परिणामस्वरूप, 12 जून, 2023 को 5 मिलियन यूरो या लगभग 5.7 मिलियन अमेरिकी डॉलर का जुर्माना लगाया गया।

**भारत में क्या होगा?**

- **प्रासंगिक डीपीडीपीए प्रावधान:** डीपीडीपीए की धारा 11 के अंतर्गत, डीपी डीएफ से अपने पीडी तक पहुंच का अनुरोध कर सकता है। ऐसा अनुरोध प्राप्त होने पर, डीएफ को संसाधित किए जा रहे पीडी और की गई प्रसंस्करण गतिविधियों का सारांश प्रदान करना अनिवार्य है। इसके अतिरिक्त, कुछ शर्तों के अधीन, फिड्यूशरी को (i) डीएफ और डीपीआर की पहचान भी प्रदान करनी होगी जिनके साथ डेटा साझा किया गया है, साथ ही साझा किए गए डेटा का विवरण; और (ii) कोई अन्य प्रासंगिक जानकारी।

- **जुर्माना:** उपरोक्त मामले के तथ्यों को ध्यान में रखते हुए, डेटा एक्सेस अनुरोधों को पूरा करने में विफलता के कारण प्रत्येक उल्लंघन पर 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है।

# अवधारणा 8: डेटा उल्लंघन

डीपीडीपीए और डीपीडीपी नियम, पीडी उल्लंघन के मामलों में विभिन्न अनुपालन आवश्यकताओं का प्रावधान करते हैं।

## 1. कानून क्या कहता है?

धारा 8(6) के अंतर्गत, डीएफ को डीपीबीआई और प्रत्येक प्रभावित डीपी को "पीडी उल्लंघन" की सूचना प्रदान करनी चाहिए।

नियम 7 आगे स्पष्ट करता है कि सूचनाएं

- "सर्वोत्तम ज्ञान" के अनुरूप बनें
- उपयोगकर्ता खातों या संचार के किसी अन्य माध्यम से भेजा जाना चाहिए।

## 2. पीडी उल्लंघन क्या होता है?

धारा 2(यू) के अंतर्गत, पी.डी. उल्लंघन में (i) पी.डी. का अनधिकृत प्रसंस्करण, या (ii) आकस्मिक प्रकटीकरण, अधिग्रहण, साझाकरण, उपयोग, परिवर्तन, विनाश, या पी.डी. तक पहुंच की हानि शामिल है, जो इसकी गोपनीयता, अखंडता, या उपलब्धता को प्रभावित करती है।

यह परिभाषा अत्यंत व्यापक है और इसके कार्यान्वयन में कठिनाइयाँ उत्पन्न होंगी।

## 3. उल्लंघन की सूचना डीपी को किस प्रकार दी जाए?

नियम 7 के अनुसार, डीएफ को प्रत्येक प्रभावित डीपी को "बिना देरी के" सूचित करना आवश्यक है, जिसमें निम्नलिखित विवरण शामिल होंगे:

- उल्लंघन का विवरण (प्रकृति, दायरा, समय और स्थान)
- ऐसे डीपी से जुड़े परिणाम
- किए गए शमन उपायों
- डी.पी. के लिए अनुशंसित सुरक्षा प्रावधान
- अधिकृत कर्मचारियों की संपर्क जानकारी

## 4. डीपीबी को सूचित करने की प्रक्रिया क्या है?

नियम 7 के अनुसार, डीएफ को उल्लंघन की प्रकृति, सीमा, समय, स्थान और संभावित प्रभाव सहित, डीपीबीआई को "तत्काल" रिपोर्ट करनी चाहिए।

डीएफ को एक अद्यतन रिपोर्ट भेजनी होगी जिसमें (क) उल्लंघन की विस्तृत जानकारी, (ख) घटना, परिस्थितियों और कारण का सारांश, (ग) जोखिम कम करने के लिए उठाए गए कदम, (घ) जिम्मेदार पक्ष, (ङ) भविष्य के उल्लंघनों को रोकने के लिए उपाय, और (च) प्रभावित डीपीएस को दी गई अधिसूचनाओं की स्थिति डीपीबीआई को "72 घंटे के भीतर" (या अनुमति मिलने पर अधिक समय के भीतर) सूचित करनी होगी।

उप-खण्ड (एफ) का तात्पर्य है कि डीपी को 72 घंटों के भीतर, अर्थात् डीपीबीआई को उल्लंघन की विस्तृत रिपोर्ट प्रदान करने से पूर्व, सूचित किया जाना चाहिए।

## 5. यदि डीएफ सूचना प्रदान करने में असफल रहते हैं, तो क्या परिणाम होगा?

डीपीडीपीए की अनुसूची के अनुसार धारा 33(1) के तहत, यदि कोई डीएफ प्रभावित डीपी या डीपीबी पीडी उल्लंघन के बारे में सूचित करने में असफल रहता है, तो उस पर 2 बिलियन रुपये या लगभग 23 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जाएगा।

## 6. चिंताएं

- **अनुपालन की लागत:** कुल मिलाकर, डीपीडीपीए और डीपीडीपी नियमों के तहत अनुपालन की आवश्यकताएँ अत्यधिक व्यापक हैं। जबकि बड़े संगठनों के पास अनुपालन के लिए पर्याप्त संसाधन होते हैं, स्टार्ट-अप और अन्य छोटी कंपनियों को वित्तीय चुनौतियों का सामना करना पड़ सकता है।

- **क्षेत्रीय रिपोर्टिंग आवश्यकताएँ:** उल्लंघन की प्रकृति के अनुसार, डीएफ को 6 घंटे के भीतर CERT-In और अन्य क्षेत्रीय नियामकों (सेबी, आईआरडीए, आरबीआई, आदि) को सूचित करने की आवश्यकता हो सकती है। विभिन्न रिपोर्टिंग मानकों और समयसीमाओं को ध्यान में रखते हुए यह प्रक्रिया जटिल हो सकती है।

- **72 घंटे की रिपोर्टिंग समय-सीमा:** डीपी और डीपीबीआई को सूचित किए जाने वाले आवश्यक विवरणों को ध्यान में रखते हुए, इतनी संक्षिप्त समय-सीमा में अनुपालन करना कई चुनौतियों का सामना करेगा।

- **अस्पष्ट अभिव्यक्तियों का समावेश:** "आकस्मिक प्रकटीकरण" जैसे कुछ शब्द अत्यंत अस्पष्ट हैं। यह स्पष्ट नहीं है कि क्या डीएफ को ऐसे मामलों में सूचित करने की आवश्यकता होगी, जहां कोई अनधिकृत कर्मचारी किसी सहकर्मी के लैपटॉप के पास से गुजरने में सफल हो जाता है, जिसमें कुछ पीडी प्रदर्शित हो रहा है।

- **विस्तृत रिपोर्टिंग आवश्यकताएँ:** डीपीडीपीए के तहत सभी उल्लंघनों की रिपोर्टिंग अनिवार्य है, चाहे डेटा प्रदाता को कोई भी नुकसान हुआ हो। इससे डीएफ और डेटा प्रोसेसिंग बॉडी पर अतिरिक्त बोझ पड़ सकता है। डेटा प्रदाताओं को बार-बार उल्लंघन नोटिस प्राप्त होने से भी असुविधा हो सकती है, जो दीर्घकालिक में उनके विश्वास को कमजोर कर सकती है और उन्हें अपनी सहमति देने से हतोत्साहित कर सकती है। इसका डेटा-संचालित व्यवसायों पर महत्वपूर्ण प्रभाव पड़ सकता है।

- **डीपीबीआई की बैंडविड्थ:** रिपोर्ट किए गए पीडी उल्लंघनों की संख्या के संदर्भ में, डीपीबी के पास सभी रिपोर्टों का प्रभावी मूल्यांकन करने के लिए पर्याप्त मानव संसाधन या बजट नहीं हो सकता है। इसके परिणामस्वरूप, अधिक व्यय के कारण डीपीबीआई द्वारा अधिक दंड लगाया जा सकता है।

**आगे बढ़ने का मार्ग**

डीएफ को (i) उल्लंघन रिपोर्टिंग आवश्यकताओं का प्रबंधन करने के लिए समर्पित टीमों का गठन करना होगा, (ii) उन्नत सुरक्षा प्रणालियों और अनुपालन उपकरणों में निवेश करना होगा, (iii) प्रभाव को कम करने के लिए सतर्कता और जवाबदेही को बढ़ाकर एक सक्रिय दृष्टिकोण अपनाना होगा, (iv) डेटा उल्लंघन/साइबर सुरक्षा बीमा में निवेश करना होगा, (v) रिपोर्टिंग में मानक संचालन प्रक्रियाओं (एसओपी) को शामिल करना होगा, और (vi) आईटी और कानूनी टीमों के बीच उचित समन्वय सुनिश्चित करना होगा।

# क्या होगा यदि "व्यक्तिगत डेटा उल्लंघन" के ये जीडीपीआर मामले भारत में घटित हों?

## जीडीपीआर के अंतर्गत व्यक्तिगत डेटा उल्लंघन की परिभाषा क्या है?

जीडीपीआर का अनुच्छेद 4(12) पीडी उल्लंघन को "सुरक्षा का उल्लंघन" के रूप में परिभाषित करता है, जिसके परिणामस्वरूप प्रेषित, संग्रहीत या अन्यथा संसाधित व्यक्तिगत डेटा का आकस्मिक या अवैध विनाश, हानि, परिवर्तन, अनधिकृत प्रकटीकरण या पहुंच हो सकती है।

**डीपीडीपीए के अनुसार पीडी का उल्लंघन**

डीपीडीपीए की धारा 2(यू) पीडी उल्लंघन को "व्यक्तिगत डेटा के किसी भी अनधिकृत प्रसंस्करण या आकस्मिक प्रकटीकरण, अधिग्रहण, साझाकरण, उपयोग, परिवर्तन, विनाश या व्यक्तिगत डेटा तक पहुंच की हानि के रूप में परिभाषित करती है, जो व्यक्तिगत डेटा की गोपनीयता, अखंडता या उपलब्धता से समझौता करती है।"

## पी.डी. उल्लंघन के मामले में नियंत्रक/न्यायाधीश को क्या करना चाहिए?

### जीडीपीआर

**डीएस को अधिसूचना:** अनुच्छेद 34 के साथ अनुच्छेद 33(3) के अनुसार, जहां पीडी उल्लंघन के परिणामस्वरूप प्राकृतिक व्यक्तियों के अधिकारों और स्वतंत्रता को उच्च जोखिम होने की संभावना है, नियंत्रक को प्रभावित डीएस को बिना किसी देरी के स्पष्ट और सरल भाषा का उपयोग करके सूचित करना चाहिए, जिसमें (ए) डेटा संरक्षण अधिकारी या अधिकृत संपर्क का नाम और विवरण; (बी) उल्लंघन के संभावित परिणाम; और (सी) शमन उपाय शामिल हैं।

**पर्यवेक्षी प्राधिकरण (एसए) को अधिसूचना:** अनुच्छेद 33 के अंतर्गत, जब पीडी उल्लंघन से प्राकृतिक व्यक्तियों के अधिकारों और स्वतंत्रता को खतरा होने की संभावना हो, तो नियंत्रक को बिना किसी देरी के, और जहां संभव हो, जानकारी प्राप्त होने के 72 घंटों के भीतर सूचित करना चाहिए। इसमें (ए) उल्लंघन की प्रकृति, प्रभावित डेटा विषयों और रिकॉर्ड की श्रेणियों तथा अनुमानित संख्या शामिल होनी चाहिए; और (बी) डीएस को दी गई जानकारी, जैसा कि पूर्व में उल्लेखित है। इसके अतिरिक्त, नियंत्रक को उल्लंघन, उसके प्रभाव और किए गए उपचारात्मक उपायों को इस प्रकार दस्तावेजित करना चाहिए कि एसए इसकी सत्यापन कर सके।

### डीपीडीपीए

**डी.पी. को अधिसूचना:** नियम 7(1) के अंतर्गत धारा 8(6) के अनुसार, डीएफ को प्रत्येक प्रभावित डीपी को बिना किसी देरी के निम्नलिखित सूचनाएँ प्रदान करना आवश्यक है: (क) उल्लंघन का विवरण (प्रकृति, सीमा, समय और स्थान), (ख) प्रासंगिक परिणाम, (ग) किए गए शमन उपाय, (घ) अनुशंसित सुरक्षा उपाय, (ङ) अधिकृत कर्मियों की संपर्क जानकारी।

**डीपीबीआई को अधिसूचना:** नियम 7(2) के साथ धारा 8(6) में उल्लेख किया गया है कि डीएफ को बिना किसी देरी के डीपीबीआई को उल्लंघन और उसके संभावित प्रभाव का विवरण प्रस्तुत करना चाहिए। इसके अतिरिक्त, 72 घंटों के भीतर एक अद्यतन रिपोर्ट प्रदान की जानी चाहिए जिसमें (ए) उल्लंघन की अद्यतन जानकारी, (बी) घटना, परिस्थितियों और कारण के विस्तृत तथ्य, (सी) जोखिम शमन उपाय, (डी) जिम्मेदार पक्ष, (ई) उपचारात्मक उपाय, और (एफ) प्रभावित डीपी को अधिसूचनाओं की स्थिति शामिल हो।

## दंड

### जीडीपीआर

गंभीर उल्लंघनों के लिए, पिछले वित्तीय वर्ष से 20 मिलियन यूरो या लगभग 24 मिलियन अमेरिकी डॉलर या कंपनी के कुल वैश्विक कारोबार का 4%, जो भी अधिक हो, का जुर्माना लगाया जाएगा। कम गंभीर उल्लंघनों के लिए, 10 मिलियन यूरो या लगभग 12 मिलियन अमेरिकी डॉलर या पिछले वित्तीय वर्ष से कुल वैश्विक कारोबार का 2%, जो भी अधिक हो।

### डीपीडीपीए

यदि कोई डीएफ प्रभावित डीपी या डीपीबीआई पीडी उल्लंघन के बारे में सूचित करने में असफल रहता है, तो 2 बिलियन रुपये या लगभग 23.5 मिलियन अमेरिकी डॉलर तक का जुर्माना लगाया जा सकता है। इसके अतिरिक्त, डीपीबीआई पीडी उल्लंघन को रोकने के लिए उचित सुरक्षा उपाय करने में विफल रहने पर 2.5 बिलियन रुपये या लगभग 29 मिलियन अमेरिकी डॉलर तक का जुर्माना लगा सकता है।

## मुख्य निर्णय

### 1. स्पेन - कैरेफोर (2025)

- **पृष्ठभूमि:** फ्रांसीसी खुदरा दिग्गज कैरेफोर की सहायक कंपनी कैरेफोर स्पेन ने जनवरी और सितंबर 2023 के बीच पांच डेटा उल्लंघनों की सूचना दी, जो सभी क्रेडेंशियल स्टफिंग (एक साइबर हमला जिसमें चोरी किए गए उपयोगकर्ता नाम-पासवर्ड जोड़े का उपयोग स्वचालित लॉगिन प्रयासों में किया जाता है) के माध्यम से क्लाइंट के खातों तक अवैध पहुंच से उत्पन्न हुए थे। उल्लेखनीय है कि कंपनी को अक्टूबर 2022 की शुरुआत में पहले उल्लंघन के बारे में जानकारी मिली थी, लेकिन जनवरी 2023 तक इसकी रिपोर्ट करने में विफल रही। इसके अतिरिक्त, कैरेफोर ने प्रभावित ग्राहकों को पहले दो उल्लंघनों के बारे में सूचित नहीं किया। कैरेफोर ने यह तर्क किया कि उसने अपने ग्राहकों को तीसरे उल्लंघन के बारे में सूचित किया था, लेकिन फिर भी, संचार में केवल यह उल्लेख किया गया कि पासवर्ड को रीसेट करना आवश्यक था और यह बताया गया कि इसे कैसे किया जा सकता है।

- **निष्कर्ष:** स्पैनिश डेटा प्रोटेक्शन अथॉरिटी (**स्पैनिश डीपीए**) ने मई 2023 में एक जांच आरंभ की। जबकि कैरेफोर ने केवल 974 खातों के प्रभावित होने का दावा किया, स्पेनिश डीपीए ने लगभग 119,000 समझौता किए गए खातों की पहचान की। यह निष्कर्ष निकाला गया कि हमलावरों के पास ग्राहकों के व्यक्तिगत डेटा तक पहुंच हो सकती है, जिसमें उनके नाम, संपर्क विवरण और पते शामिल हैं। इसने कैरेफोर को सक्रिय सुरक्षा उपाय करने में विफल रहने के लिए अनुच्छेद 5(1)(एफ), अनुच्छेद 24(1), और अनुच्छेद 32 के उल्लंघन का दोषी ठहराया। विशेष रूप से, दो-कारक प्रमाणीकरण केवल पांचवें उल्लंघन के बाद लागू किया गया था। इसके अतिरिक्त, कंपनी अनुच्छेद 34 का उल्लंघन करते हुए निर्धारित तरीके से उल्लंघन के बारे में डेटा सुरक्षा अधिकारी को सूचित करने में असफल रही। इसके अलावा, अनुच्छेद 33 का उल्लंघन करते हुए प्रभावित व्यक्तियों की वास्तविक संख्या की रिपोर्ट एसए को प्रस्तुत करने में असफल रही। तदनुसार, 14 मार्च 2025 को निम्नलिखित के लिए जुर्माना लगाया गया: (ए) अनुच्छेद 5 (1) (एफ) का उल्लंघन करने पर 2 मिलियन यूरो या लगभग 2.4 मिलियन अमरीकी डालर; (बी) अनुच्छेद 32 का उल्लंघन करने पर 1 मिलियन यूरो या लगभग 1.2 मिलियन अमरीकी डालर; और अनुच्छेद 34 का उल्लंघन करने पर 200,000 यूरो या लगभग 240,000 अमरीकी डालर। इसके अतिरिक्त, कंपनी को डीएस को उल्लंघन की सूचना देने के लिए निर्देशित किया गया।

**भारत में क्या होगा?**

- **विश्लेषण और जुर्माना:** इस मामले में, अनधिकृत तीसरे पक्ष ने ग्राहक खातों तक पहुँच प्राप्त की। डीपीडीपीए के अंतर्गत, इस प्रकार का अनधिकृत उपयोग धारा 2(u) के तहत व्यक्तिगत डेटा उल्लंघन के रूप में वर्गीकृत किया जाता है। तदनुसार, कंपनी धारा 8(5) का उल्लंघन करेगी, क्योंकि यह व्यक्तिगत डेटा की सुरक्षा के लिए उचित सुरक्षा उपाय करने में असफल रही है, जिसके लिए प्रति उल्लंघन 2.5 बिलियन रुपये या लगभग 29 मिलियन अमरीकी डॉलर तक का जुर्माना लगाया जा सकता है। इसके अतिरिक्त, चूंकि कंपनी उल्लंघन के संबंध में डीपी को सूचित करने में विफल रही, इसलिए इसे धारा 8(6) का उल्लंघन माना जाएगा। इसके लिए, 2 बिलियन रुपये या लगभग 23.5 अमरीकी डॉलर प्रति उल्लंघन तक का अतिरिक्त जुर्माना लगाया जा सकता है।

**मुख्य निष्कर्ष**

मजबूत और सक्रिय डेटा सुरक्षा नियंत्रणों को लागू करना और बनाए रखना (जैसे बहु-कारक प्रमाणीकरण, समय पर घुसपैठ का पता लगाना, गहन उल्लंघन प्रतिक्रिया) तथा सभी डीपीडीपीए रिपोर्टिंग दायित्वों को पूरा करना, जिसमें उल्लंघन की स्थिति में डीपीबीआई और प्रभावित व्यक्तियों को तुरंत सूचित करना शामिल है।

## 2. आयरलैंड - मेटा (2024)

- **पृष्ठभूमि:** जुलाई 2018 में, मेटा प्लेटफ़ॉर्म आयरलैंड लिमिटेड (**एमपीआईएल**) ने Facebook पर वीडियो अपलोड करने की सुविधा प्रारंभ की। इसके पश्चात, Facebook के 'व्यू ऐज़' फ़ंक्शन ने उपयोगकर्ताओं को अपनी प्रोफ़ाइल का पूर्वावलोकन करने की अनुमति दी, जैसा कि यह किसी अन्य उपयोगकर्ता को दिखाई देगा। Facebook के वीडियो अपलोडर के साथ उपयोग किए जाने पर, प्रणाली ने एक "उपयोगकर्ता टोकन" उत्पन्न किया, जिसने तीसरे पक्ष को उस उपयोगकर्ता की संपूर्ण प्रोफ़ाइल तक पहुँचने में सक्षम बनाया। इसके परिणामस्वरूप, वैश्विक स्तर पर लगभग 29 मिलियन Facebook खाते प्रभावित हुए, जिनमें EU/EEA में 3 मिलियन शामिल थे। MPIL और उसके अमेरिकी पैरेंट द्वारा उल्लंघन की पहचान के बाद इसे शीघ्र ही सुधार लिया गया।

- **निष्कर्ष:** आयरिश डेटा संरक्षण आयोग (**आयरिश डीपीसी**) ने दो जांच आरंभ की और एमपीआईएल को लाखों उपयोगकर्ताओं के नाम, ईमेल, फोन नंबर, जन्मतिथि, लिंग, बच्चों के डेटा आदि सहित पीडी तक अनधिकृत पहुंच की अनुमति देने के लिए उत्तरदायी पाया। इस प्रकार, 17 दिसंबर 2024 को निम्नलिखित जुर्माना लगाया गया: (ए) अनुच्छेद 33 (3) (अपूर्ण उल्लंघन अधिसूचना) के उल्लंघन के लिए 8 मिलियन यूरो या लगभग 9.5 मिलियन अमरीकी डॉलर; (बी) अनुच्छेद 33 (5) (अपर्याप्त उल्लंघन दस्तावेज) के उल्लंघन के लिए 3 मिलियन यूरो या लगभग 3.6 मिलियन अमरीकी डॉलर; (सी) अनुच्छेद 25(1) (डिज़ाइन द्वारा डेटा सुरक्षा लागू करने में विफलता) के उल्लंघन के लिए 130 मिलियन यूरो या लगभग 154 मिलियन अमेरिकी डॉलर; (डी) अनुच्छेद 25(2) (डिफ़ॉल्ट रूप से डेटा न्यूनतमीकरण सुनिश्चित करने में विफलता) के उल्लंघन के लिए 110 मिलियन यूरो या लगभग 130 मिलियन अमेरिकी डॉलर। कुल मिलाकर, 251 मिलियन यूरो या लगभग 295 मिलियन अमेरिकी डॉलर।

**भारत में क्या होगा?**

- **विश्लेषण और जुर्माना:** यदि यह मामला भारत में घटित हुआ होता, तो एमपीआईएल को उचित सुरक्षा उपायों का उपयोग करके अपने कब्जे में पीडी की रक्षा करने के लिए बाध्य होना पड़ता। 'व्यू एज़' और वीडियो अपलोड सुविधाओं का संयोजन तीसरे पक्ष द्वारा उपयोगकर्ताओं के पीडी के अनधिकृत उपयोग को सक्षम करता था। यह डीपीडीपीए की धारा 2(u) के तहत पीडी उल्लंघन के रूप में योग्य है। परिणामस्वरूप, डीपीबीआई द्वारा Facebook पर प्रति उल्लंघन 2.5 बिलियन रुपये या लगभग 29 मिलियन अमरीकी डॉलर का जुर्माना लगाया जा सकता है। इसके अतिरिक्त, यदि MPIL डीपी और डीपीबीआई को अपने उल्लंघन अधिसूचना में ड्राफ्ट नियम 7 के अनुसार आवश्यक जानकारी प्रदान करने में विफल रहता, तो डीपीबीआई द्वारा प्रति उल्लंघन 2 बिलियन रुपये या लगभग 23.5 मिलियन अमरीकी डॉलर तक का जुर्माना लगाया जा सकता था।

**मुख्य निष्कर्ष**

सुनिश्चित करें कि डेटा सुरक्षा को शुरू से ही सिस्टम डिज़ाइन में शामिल किया गया है (डिज़ाइन द्वारा गोपनीयता, डेटा न्यूनीकरण), और लॉन्च से पहले सुविधाओं को सख्ती से मान्य करें ताकि एक्सेस-कंट्रोल या टोकन के दुरुपयोग को रोका जा सके जो बड़े पैमाने पर उल्लंघनों का कारण बन सकता है।

### 3. स्पेन - वोडाफोन (2024)

- **पृष्ठभूमि:** 14 दिसंबर 2022 को, एक डीएस ने वोडाफोन स्पेन के खिलाफ स्पेनिश डीपीए में शिकायत दर्ज की, जिसमें आरोप लगाया गया कि एक तीसरे पक्ष ने उसकी सहमति के बिना, डुप्लीकेट सिम कार्ड का अनुरोध किया। यह डीएस के खाते में लॉग इन करके और बिलिंग पते से भिन्न पते पर डिलीवरी का अनुरोध करके किया गया था। जवाब में, वोडाफोन स्पेन ने तर्क किया कि तीसरे पक्ष ने सोशल इंजीनियरिंग के माध्यम से प्राप्त वैध एक्सेस क्रेडेंशियल्स का उपयोग किया और जब सही लॉगिन विवरण प्रदान किए गए तो पहचान को उचित रूप से सत्यापित नहीं कर सका। इसके अतिरिक्त, इसने कहा कि तीसरे पक्ष ने डिलीवरी को पूरा करने के लिए लॉजिस्टिक्स प्रदाता को एक नकली आईडी प्रस्तुत की थी। उल्लेखनीय है कि वोडाफोन स्पेन सिम कार्ड के उपयोग के लिए आवश्यक किसी भी हस्ताक्षर या सक्रियण कॉल की रिकॉर्डिंग का प्रमाण देने में असफल रहा।

- **निष्कर्ष:** स्पेनिश डीपीए ने पाया कि वोडाफोन स्पेन प्रतिरूपण को रोकने के लिए आवश्यक उपाय लागू करने में असफल रहा है। इसने माना कि, एक बड़े पैमाने पर डीसी के रूप में, वोडाफोन स्पेन से ऐसे जोखिमों के खिलाफ सुरक्षा उपायों की अपेक्षा की जाती थी। इसके अतिरिक्त, वोडाफोन स्पेन अपनी सुरक्षा नीति के अनुपालन को प्रदर्शित करने में विफल रहा, क्योंकि यह सत्यापन कॉल रिकॉर्डिंग या डिलीवरी हस्ताक्षर प्रस्तुत करने में असमर्थ रहा। तदनुसार, 5 मई, 2024 को, डीपीए ने अनुच्छेद 6(1) जीडीपीआर के तहत डेटा सब्जेक्ट के व्यक्तिगत डेटा को वैध रूप से संसाधित करने में विफलता के लिए वोडाफोन स्पेन के वार्षिक कारोबार के आधार पर 200,000 यूरो या लगभग 240,000 अमरीकी डॉलर का जुर्माना लगाया।

**भारत में क्या होगा?**

- **विश्लेषण और जुर्माना:** उपरोक्त मामले के तथ्यों को लागू करते हुए, एक तीसरे पक्ष ने डुप्लिकेट सिम कार्ड के लिए अनुरोध किया, जिसका अर्थ है कि डीपी के क्रेडेंशियल और पासवर्ड तीसरे पक्ष के पास उपलब्ध थे, जो अनधिकृत उपयोग के समान है और धारा 2 (यू) की परिभाषा के अंतर्गत आता है। तदनुसार, डीपीबीआई उचित सुरक्षा उपायों का उपयोग करके अपने कब्जे में पीडी की सुरक्षा सुनिश्चित करने में विफल रहने के लिए 2.5 बिलियन रुपये या लगभग 29 मिलियन अमेरिकी डॉलर प्रति उल्लंघन तक का जुर्माना लगा सकता है। इसके अतिरिक्त, डीपी की सहमति का उपयोग निर्दिष्ट उद्देश्य के अलावा किसी अन्य उद्देश्य के लिए किया गया था। परिणामस्वरूप, प्रति उल्लंघन 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर का अतिरिक्त जुर्माना लगाया जा सकता है।

**मुख्य निष्कर्ष**

कंपनियाँ अक्सर मानती हैं कि गोपनीयता अनुपालन केवल तकनीकी और संगठनात्मक उपायों के कार्यान्वयन तक सीमित है। हालाँकि, गोपनीयता अनुपालन के लिए एक समग्र पारिस्थितिकी तंत्र की आवश्यकता होती है, जो केवल नीतियों से अधिक है। इसके लिए कंपनी के दैनिक संचालन में गोपनीयता के प्रति सचेत दृष्टिकोण अपनाना आवश्यक है। प्रत्येक क्रिया को गोपनीयता के सिद्धांतों के अनुरूप होना चाहिए।

## 4. क्रोएशिया - ईओएस मैट्रिक्स डी.ओ.ओ. (2023)

- **पृष्ठभूमि:** 22 मार्च, 2023 को क्रोएशियाई पर्यवेक्षी प्राधिकरण (**क्रोएशियाई एसए**) के समक्ष एक गुमनाम याचिका प्रस्तुत की गई, जिसमें ईओएस मैट्रिक्स डीओओ द्वारा ऋण वसूली एजेंसी के माध्यम से पीडी की अनधिकृत प्रोसेसिंग का आरोप लगाया गया। शिकायत के साथ एक यूएसबी स्टिक भी संलग्न थी, जिसमें 294 बच्चों सहित 181,641 व्यक्तियों के पीडी शामिल थे। ये व्यक्ति विभिन्न ऋण संस्थानों के देनदार थे, जिनका ऋण ईओएस ने सेशन अनुबंधों के माध्यम से प्राप्त किया था। डेटा में नाम, जन्म तिथि और व्यक्तिगत पहचान संख्याएँ शामिल थीं।

- **निष्कर्ष:** अपनी जांच के पश्चात, क्रोएशियाई एसए ने यह निष्कर्ष निकाला कि ईओएस ने जीडीपीआर के अनुच्छेद 32 के तहत पर्याप्त तकनीकी उपायों को लागू करने में विफलता दर्शाई है। विशेष रूप से, कंपनी के मुख्य डेटाबेस में लगभग 370,000 व्यक्तियों के व्यक्तिगत डेटा के होने के कारण, असामान्य गतिविधियों जैसे डेटा पुनर्प्राप्ति की संख्या में वृद्धि, सिस्टम के बाहर डेटा स्थानांतरण, या समझौता किए गए उपयोगकर्ता पहुंच का पता लगाने की क्षमता का अभाव था। इसके अतिरिक्त, ईओएस ने जीडीपीआर के अनुच्छेद 6(1) के तहत वैध कानूनी आधार के बिना व्यक्तिगत डेटा को संसाधित किया, जिसमें ऐसे व्यक्तियों का डेटा भी शामिल था जो देनदार नहीं थे। इसके अलावा, मई 2018 से अक्टूबर 2020 तक कंपनी की गोपनीयता नीतियों में गलत तरीके से कहा गया कि स्वास्थ्य डेटा का संसाधन नहीं किया जा रहा था, जो अनुच्छेद 12(1), 13(1), और 13(2) के तहत पारदर्शिता दायित्वों का उल्लंघन करता है। इसके अलावा, यह पाया गया कि मई 2018 और जनवरी 2019 के बीच, ईओएस ने बिना किसी वैध आधार के 49,850 व्यक्तियों की टेलीफोन बातचीत रिकॉर्ड की, जिसके परिणामस्वरूप जीडीपीआर के अनुच्छेद 6(1) और 5(2) का और उल्लंघन हुआ। परिणामस्वरूप, 5 अक्टूबर, 2023 को, क्रोएशियाई एसए ने जीडीपीआर के अनुच्छेद 5, 6, 9, 12, 13 और 32 के उल्लंघन के लिए 5,470,000 यूरो या लगभग 6.5 मिलियन अमेरिकी डॉलर का जुर्माना लगाया।

**भारत में क्या होगा?**

- **विश्लेषण और जुर्माना:** भारतीय कानून के अंतर्गत, कंपनियों के लिए उचित सुरक्षा उपायों का एक सेट लागू करना अनिवार्य है। चूंकि, EOS इन उपायों को अपनाने में विफल रहा, इसे धारा 8(5) का उल्लंघन माना जाएगा, जिसके तहत प्रति उल्लंघन 2.5 बिलियन रुपये या लगभग 29 मिलियन अमेरिकी डॉलर का जुर्माना लगाया जाएगा। इसके अतिरिक्त, धारा 4(1) केवल (ए) सहमति या (बी) वैध उपयोग के आधार पर पीडी के प्रसंस्करण की अनुमति देती है। चूंकि EOS के पास पीडी के प्रसंस्करण के लिए कोई वैध कानूनी आधार नहीं था, यह प्रति उल्लंघन 500 मिलियन रुपये या लगभग 6 मिलियन अमेरिकी डॉलर के अतिरिक्त जुर्माने के लिए उत्तरदायी होगा। इसके अलावा, डीपीडीपीए बच्चों के डेटा को संसाधित करते समय कंपनियों पर अतिरिक्त दायित्व लगाता है। ऐसा करने में किसी भी विफलता के लिए प्रति उल्लंघन 2 बिलियन रुपये या लगभग 23.5 मिलियन अमेरिकी डॉलर का अतिरिक्त जुर्माना लगाया जाता है।

**मुख्य निष्कर्ष**

यह सुनिश्चित करें कि केवल वैध आधार पर संसाधित डेटा एकत्रित किया जाए और सुरक्षित रूप से रखा जाए, विशेष रूप से जब इसमें संवेदनशील स्वास्थ्य जानकारी शामिल हो। इसके साथ ही, विसंगतियों का पता लगाने, अनधिकृत पहुंच या निष्कासन को रोकने, और डेटा प्रबंधन के प्रति पूर्ण पारदर्शिता सुनिश्चित करने के लिए मजबूत तकनीकी और संगठनात्मक उपायों (टीओएम) को लागू करें।

## 5. जर्मनी - एचएंडएम (2020)

- **पृष्ठभूमि:** एचएंडएम ने नूर्नबर्ग में एक सेवा केंद्र का संचालन किया। कम से कम 2014 से, इसने अपने कुछ कर्मचारियों के निजी जीवन के विस्तृत रिकॉर्ड बनाए रखे, जिसमें नोट्स स्थायी रूप से नेटवर्क ड्राइव पर संग्रहीत थे। कंपनी ने "वेलकम बैक टॉक्स" के माध्यम से जानकारी दर्ज की, जिसमें प्रबंधन ने छुट्टियों के अनुभवों, बीमारियों आदि का विवरण संकलित किया। इसके अतिरिक्त, आमने-सामने या अनौपचारिक गलियारे की बातचीत के माध्यम से जानकारी एकत्र की गई, जहाँ प्रबंधकों ने कर्मचारियों के जीवन के बारे में व्यक्तिगत विवरण, जैसे कि पारिवारिक मुद्दे, धार्मिक विश्वास आदि, एकत्र किए। कुछ मामलों में, डेटा को डिजिटल रूप से संग्रहीत किया गया और कंपनी भर में लगभग 50 प्रबंधकों के लिए सुलभ बनाया गया। इसके अलावा, कंपनी ने कर्मचारी प्रोफाइल बनाने के लिए एकत्रित डेटा का उपयोग किया, जिससे उन्हें रोजगार निर्णय लेने में सहायता मिली। अक्टूबर 2019 में, एक कॉन्फ़िगरेशन त्रुटि ने इन व्यक्तिगत रिकॉर्ड को कई घंटों तक कंपनी-व्यापी सुलभ बना दिया। इसके परिणामस्वरूप, जर्मन डेटा प्रोटेक्शन अथॉरिटी (जर्मन डीपीए) द्वारा एक जांच शुरू की गई।

- **निष्कर्ष:** अपनी जांच के पश्चात, जर्मन डीपीए ने यह निष्कर्ष निकाला कि एचएंडएम की कार्यप्रणाली ने कर्मचारियों के गोपनीय डेटा की सुरक्षा के प्रति गंभीर लापरवाही प्रदर्शित की। इसके परिणामस्वरूप, 2 अक्टूबर, 2020 को 35.3 मिलियन यूरो या लगभग 42 मिलियन अमेरिकी डॉलर का जुर्माना लगाया गया।

**भारत में क्या होगा?**

- **विश्लेषण और दंड:** वर्तमान मामले के तथ्यों को लागू करते हुए, "रोजगार" डीपीडीपीए की धारा 7(i) के तहत पीडी प्रक्रिया का एक वैध आधार है। हालांकि, एचएंडएम के मामले में, एकत्र किए गए डेटा का प्रकार अत्यधिक व्यापक था और इसे "रोजगार के उद्देश्य" के लिए एकत्र किए गए पीडी के दायरे में नहीं कहा जा सकता था। इसके अतिरिक्त, किसी भी कर्मचारी की सहमति प्राप्त नहीं की गई थी।

  इस प्रकार, एचएंडएम के पास व्यक्तिगत डेटा (पीडी) को इकट्ठा करने और संग्रहीत करने का कोई वैध आधार नहीं था। इसके अतिरिक्त, धारा 2(यू) के अनुसार, पीडी का कोई भी "अनधिकृत प्रसंस्करण" पीडी उल्लंघन के रूप में माना जाता है। इसके अलावा, एकत्र की गई पीडी को 50 प्रबंधकों के लिए और बाद में कंपनी भर में सुलभ बनाया गया था, जिससे पीडी की "गोपनीयता" से समझौता हुआ। परिणामस्वरूप, उचित सुरक्षा उपायों को लागू करने में विफलता के लिए डेटा संरक्षण ब्यूरो (डीपीबीआई) द्वारा 2.5 बिलियन रुपये या लगभग 29 मिलियन अमेरिकी डॉलर प्रति उल्लंघन का जुर्माना लगाया जा सकता था।

**मुख्य निष्कर्ष**

कंपनियों को यह पुनर्मूल्यांकन करना चाहिए कि वे किस प्रकार का पीडी एकत्रित और संग्रहीत करती हैं। डेटा केवल तभी एकत्रित किया जाना चाहिए जब कोई "स्पष्ट और आवश्यक उद्देश्य" हो। प्रत्येक डेटा को उसके "उद्देश्य" से संबंधित करें और यदि "उद्देश्य" अस्पष्ट है - तो उसे एकत्रित न करें।

# अवधारणा 9: साइबर बीमा

साइबर बीमा डिजिटल जोखिमों के प्रबंधन और उनके न्यूनीकरण के लिए एक अनिवार्य उपकरण है। यह साइबर हमलों से उत्पन्न होने वाले नुकसानों के खिलाफ वित्तीय सुरक्षा प्रदान करता है, जिसमें कानूनी खर्च, नियामक दंड या डेटा पुनर्प्राप्ति लागत शामिल हैं। यह कवरेज तब अत्यंत महत्वपूर्ण हो जाता है जब ग्राहक या कर्मचारी का डेटा हैकिंग, डेटा चोरी या आकस्मिक जोखिम के कारण समझौता किया जाता है।

## किस प्रकार के नुकसान को कवर किया जाता है?

- **प्रथम-पक्ष हानियाँ:** प्रत्यक्ष वित्तीय हानियाँ, जैसे डेटा पुनर्प्राप्ति, व्यवसाय में रुकावटें, घटना प्रतिक्रियाएँ और शमन प्रयासों की लागत।
- **तृतीय-पक्ष हानियाँ:** ग्राहकों/विक्रेताओं से प्राप्त दावे, जिनमें कानूनी बचाव लागत, नियामक दंड और समझौता शामिल हैं।

## केस अध्ययन: मार्क्स एंड स्पेंसर साइबर घटना


**पृष्ठभूमि:** अप्रैल 2025 में, यूके की प्रमुख खुदरा कंपनी मार्क्स एंड स्पेंसर (M&S) को एक साइबर घटना का सामना करना पड़ा, जिसके परिणामस्वरूप ग्राहक डेटा का नुकसान हुआ और परिचालन में व्यवधान उत्पन्न हुआ। इस उल्लंघन के कारण M&S के ऑनलाइन कपड़ों के कारोबार को अस्थायी रूप से निलंबित कर दिया गया, जिससे इसके बाजार मूल्य में 750 मिलियन पाउंड की कमी आई।

निष्कर्षों से स्पष्ट हुआ कि यह घटना तकनीकी विफलता के बजाय मानव त्रुटि के कारण हुई थी, जिससे यह सिद्ध होता है कि सबसे उन्नत साइबर सुरक्षा प्रणालियाँ भी जोखिम को पूरी तरह से समाप्त नहीं कर सकती हैं।

एमएंडएस ने लगभग 300 मिलियन पाउंड की कुल हानि का अनुमान लगाया है, और व्यवधान जुलाई 2025 तक जारी रहने की संभावना है।

**साइबर बीमा पॉलिसी:** एमएंडएस की साइबर बीमा पॉलिसी से 100 मिलियन पाउंड तक के नुकसान को कवर करने की संभावना है, जबकि शेष 200 मिलियन पाउंड का भुगतान कंपनी को स्वयं करना होगा।

## साइबर बीमा पॉलिसी किस प्रकार सहायक हो सकती है?

जैसा कि एम एंड एस मामले में प्रदर्शित किया गया है, साइबर बीमा पॉलिसी साइबर घटना के पश्चात कंपनियों को वित्तीय हानि से उबरने में सहायता कर सकती है। वित्तीय कवरेज के अतिरिक्त, एक सुव्यवस्थित नीति उल्लंघन प्रतिक्रिया टीमों, वकीलों, जनसंपर्क सहायता आदि तक पहुंच प्रदान कर सकती है। ये संसाधन त्वरित पुनर्प्राप्ति और दीर्घकालिक हानि को कम करने के लिए अत्यंत महत्वपूर्ण हैं।

## आपकी साइबर बीमा आवश्यकताओं का मूल्यांकन

- कवरेज सीमा, कटौतियाँ और बहिष्करण को समझना
- संभावित घटनाओं के प्रभावों के साथ नीति लागत का संतुलन बनाएं
- कवरेज को देयता के जोखिम से मिलाएं
- व्यक्तिगत डेटा और प्रसंस्करण गतिविधियों की पहचान हेतु डेटा मैपिंग का संचालन करें
- कमियों और कमजोरियों की पहचान के लिए सुरक्षा प्रथाओं का मूल्यांकन करें
- सामान्य खतरों की पहचान करने और समान जोखिमों के मूल्यांकन के लिए उद्योग के रुझानों का विश्लेषण करें
- साइबर घटना के मामले में संभावित वित्तीय प्रभाव का आकलन करें (इसमें डीपीडीपीए और जीडीपीआर के अंतर्गत दंड भी शामिल हैं)


## सुनिश्चित करें

- डेटा मानचित्रण
- सुरक्षा प्रक्रियाओं का मूल्यांकन
- उद्योग के प्रवृत्तियों का विश्लेषण

**यह आवश्यक क्यों है?**

संगठनों को सावधानीपूर्वक कटौती योग्य राशि, कवरेज सीमा और कवर की गई घटनाओं के प्रकारों का मूल्यांकन करके अपने जोखिम प्रोफ़ाइल का आकलन करना चाहिए। यह सुनिश्चित करने के लिए कि बीमा पॉलिसी वित्तीय बोझ बने बिना सार्थक मूल्य प्रदान करती है, पॉलिसी प्रीमियम के सापेक्ष साइबर घटनाओं की संभावना और संभावित लागत का तुलनात्मक विश्लेषण करना महत्वपूर्ण है।

## सही साइबर बीमा पॉलिसी निर्धारित करने के लिए चरण

**एक आंतरिक समिति का गठन करें:** संगठन के साइबर जोखिम, व्यावसायिक प्राथमिकताओं और जोखिम उठाने की क्षमता का मूल्यांकन करने के लिए सीईओ, सीएफओ, सीआईएसओ और संबंधित विभाग प्रमुखों जैसे प्रमुख हितधारकों के साथ एक क्रॉस-फ़ंक्शनल आंतरिक समिति की स्थापना करें।

**विशेषज्ञों को शामिल करें:** जहां आवश्यक हो, व्यवसाय मूल्यांकन प्रक्रिया का समर्थन करने और प्रीमियम पर अनुकूल सौदे प्राप्त करने के लिए उपयुक्त बीमा वाहकों की पहचान करने हेतु तीसरे पक्ष के बीमा दलाल या साइबर सुरक्षा सलाहकार को शामिल किया जा सकता है।

## साइबर बीमा प्रदाता को नियुक्त करने से पूर्व ध्यान में रखने योग्य प्रमुख बिंदु

**मुख्य समावेशन का सत्यापन करें** (i) डीपीडीपीए/जीडीपीआर से संबंधित जोखिमों के लिए कवरेज; (ii) उल्लंघन प्रतिक्रिया आपूर्ति तक पहुंच; (iii) पूर्व-उल्लंघन जोखिम आकलन + घटना के पश्चात समर्थन

PSA LEGAL COUNSELLORS

### मुख्य प्रश्न

- क्या पॉलिसी सभी कवरेज क्षेत्रों के लिए पूर्ण सीमा प्रदान करती है? कृपया पुष्टि करें कि क्या पॉलिसी विभिन्न कवरेज तत्वों के लिए समर्पित सीमा या साझा/समग्र सीमा प्रदान करती है?
- क्या साइबर घटना के पश्चात प्रतिष्ठा को होने वाली हानि के लिए कोई कवरेज उपलब्ध है?
- व्यवसाय व्यवधान कवरेज के लिए प्रतीक्षा अवधि क्या है? व्यवसाय व्यवधान हानियों के लिए पॉलिसी किस हद तक उत्तरदायी है? क्या यह राजस्व की हानि, अतिरिक्त परिचालन व्यय और प्रणाली पुनर्स्थापना की लागत को शामिल करती है?
- साइबर बीमा के अंतर्गत कौन-कौन से पहलू शामिल हैं? क्या पॉलिसी में पहले पक्ष के नुकसान (जैसे साइबर जबरन वसूली और व्यापार में रुकावट) और तीसरे पक्ष की देनदारियों (गोपनीयता उल्लंघन और डेटा उल्लंघन) को शामिल किया गया है?
- क्या इसमें वार्षिक प्रीमियम समायोजन का प्रावधान है? क्या पॉलिसी जोखिम प्रोफ़ाइल में परिवर्तन या दावा इतिहास के आधार पर पुनर्संतुलन की अनुमति देती है?
- प्रत्येक प्रकार के कवरेज के लिए बीमा की सीमाएँ क्या हैं?
- क्या नीति दुष्ट कर्मचारियों या आंतरिक खतरों से उत्पन्न होने वाली हानियों को कवर करती है?
- क्या नीति में डेटा पुनर्निर्माण शामिल है, न कि केवल पुनर्स्थापना?
- क्या नोटिफिकेशन की लागत इवेंट प्रबंधन अनुभाग में शामिल की जाती है?
- क्या सोशल इंजीनियरिंग धोखाधड़ी को शामिल किया जाता है?
- पॉलिसी के अंतर्गत अपवर्जन क्या हैं?

### साइबर बीमा पॉलिसी के कुछ महत्वपूर्ण खंड इस प्रकार हैं

**प्रौद्योगिकी/पेशेवर त्रुटियाँ और चूक:** यह प्रौद्योगिकी या पेशेवर सेवाओं में हुई गलतियों या विफलताओं के कारण उत्पन्न कानूनी क्षति और दावों को शामिल करता है।

**गोपनीयता विनियामक दावे:** गोपनीयता कानून के उल्लंघन से उत्पन्न विनियामक कार्रवाइयों के कारण होने वाले जुर्माने, दंड और कानूनी व्यय को शामिल करता है।

**सुरक्षा उल्लंघन प्रतिक्रिया:** इसमें संकट प्रबंधन, फोरेंसिक जांच, कानूनी व्यय, उल्लंघन अधिसूचना और उल्लंघन के पश्चात जनसंपर्क व्यय शामिल हैं।

**मल्टीमीडिया दायित्व:** ऑनलाइन सामग्री से संबंधित दावों के लिए कवरेज प्रदान करता है, जिसके परिणामस्वरूप मानहानि, कॉपीराइट उल्लंघन, ट्रेडमार्क उल्लंघन या प्रतिष्ठा को हानि हो सकती है।

**साइबर जबरन वसूली:** साइबर जबरन वसूली या रैनसमवेयर खतरों के परिणामस्वरूप उत्पन्न होने वाली फिरौती भुगतान और संबंधित व्यय की प्रतिपूर्ति करता है।

**पीसीआई डीएसएस मूल्यांकन:** कार्डधारक डेटा से संबंधित डेटा उल्लंघन के पश्चात भुगतान कार्ड नेटवर्क द्वारा लगाए गए दंड या मूल्यांकन का भुगतान किया जाता है।

**धन या संपत्ति की हानि:** साइबर-सक्षम चोरी के कारण कंपनी या उसके ग्राहकों को हुई प्रत्यक्ष वित्तीय हानि की भरपाई।

**कानूनी व्यय (घटना के पश्चात):** इसमें कानूनी परामर्श, बचाव, और साइबर घटनाओं के समाधान या गलत आरोपों का निपटारा करने के लिए की गई कार्रवाई शामिल है।

**डेटा पुनर्स्थापना और मैलवेयर शुद्धिकरण:** यह मैलवेयर या साइबर हमलों से प्रभावित क्षतिग्रस्त डेटा को पुनर्स्थापित करने और उपकरणों को साफ करने की लागतों को शामिल करता है।

**नेटवर्क सुरक्षा दायित्व:** आपके सिस्टम/डिवाइस से उत्पन्न साइबर घटना के परिणामस्वरूप तीसरे पक्ष को होने वाली हानि के लिए भुगतान करता है।

**तृतीय-पक्ष उल्लंघन:** आपके डेटा का उल्लंघन करने वाले तृतीय पक्ष के खिलाफ दायर किए गए दावों के लिए कानूनी खर्चों की प्रतिपूर्ति करता है।

**व्यावसायिक व्यवधान और डिजिटल परिसंपत्ति की पुनर्स्थापना:** सुरक्षा उल्लंघनों या प्रणालीगत व्यवधानों के कारण डिजिटल परिसंपत्तियों की पुनर्स्थापना के लिए आय की हानि और व्यय को कवर करता है।

## साइबर बीमा का दावा प्रस्तुत करना


**पॉलिसी की शर्तों के अनुसार, दावा निपटान प्रक्रिया इस प्रकार हो सकती है**

**रिपोर्टिंग और फाइलिंग:** साइबर घटना को निर्धारित समय-सीमा के भीतर उचित नियामक प्राधिकरण को रिपोर्ट करना अनिवार्य है (उदाहरण के लिए, CERT-In के अनुसार घटना के 6 घंटे के भीतर रिपोर्ट करना आवश्यक है)। इसके अतिरिक्त, निकटतम पुलिस स्टेशन और/या स्थानीय साइबर सेल में शिकायत दर्ज कराई जानी चाहिए।

**बीमा प्रदाता को सूचित करना:** बीमा प्रदाता को घटना की सूचना अवश्य दी जानी चाहिए (आमतौर पर 1-2 दिनों के भीतर)।

**लिखित दावा प्रस्तुत करना:** दावा प्रपत्र (आमतौर पर 30 से 90 दिनों के भीतर) आवश्यक सहायक दस्तावेजों के साथ प्रस्तुत किया जाना चाहिए, जिसमें एफआईआर की प्रति, व्यय से संबंधित सभी चालान, जांच के स्क्रीनशॉट, हुई हानि का प्रमाण, किसी भी कानूनी नोटिस या अदालती सम्मन की प्रतियां आदि शामिल हैं।

**दावे का सत्यापन:** एक बार जब दावा और दस्तावेज प्रस्तुत कर दिए जाते हैं, तो बीमा कंपनी दावे के सत्यापन के लिए एक अन्वेषक या फोरेंसिक विशेषज्ञ की नियुक्ति कर सकती है।

**दावा निपटान:** दावे के सत्यापन के पश्चात, मुआवज़ा सामान्यतः विशेषज्ञ की अंतिम रिपोर्ट की तिथि से 5 से 7 दिनों के भीतर लाभार्थी के खाते में स्थानांतरित कर दिया जाता है।

**आगे बढ़ने का मार्ग**

साइबर बीमा एक महत्वपूर्ण सुरक्षा जाल है, लेकिन यह मजबूत सुरक्षा प्रथाओं या कानूनी अनुपालन का विकल्प नहीं है। संगठनों को (*i*) अपने कर्मचारियों को प्रशिक्षित करना चाहिए, क्योंकि अक्सर सबसे कमजोर कड़ी मानवीय त्रुटि होती है, (*ii*) लागू गोपनीयता कानूनों के तहत सभी दायित्वों को पूरा करना चाहिए, क्योंकि गैर-अनुपालन हमेशा दावों को अस्वीकार कर देगा, (*iii*) साइबर सुरक्षा बुनियादी ढांचे में निवेश करना चाहिए, (*iv*) अपनी साइबर बीमा पॉलिसियों की विशेषज्ञों द्वारा समीक्षा करवानी चाहिए।

# टीम

**ध्रुव सूरी**
**पार्टनर**
**d.suri@psalegal.com**

**ऋषि सेहगल**
**सीनियर एसोसिएट**
**r.sehgal@psalegal.com**

**आस्था माथुर**
**सीनियर एसोसिएट**
**a.mathur@psalegal.com**

**प्रज्ञा कृति**
**एसोसिएट**
**p.kriti@psalegal.com**

**सानिया गंडोत्रा**
**एसोसिएट**
**s.gandotra@psalegal.com**

www.psalegal.com

14 ए&बी, हंसालय
15, बाराखंभा रोड
नई दिल्ली 110 001
contact@psalegal.com