शासन में साइबर सुरक्षा व गोपनीयता

साइबर सुरक्षा और डेटा का एकीकरण डी.पी.डी.पी अधिनियम, 2023 के तहत सुरक्षा

संपादित : **मोहन दास विस्वम्**

जब किसी अस्पताल का डिजिटल सिस्टम रैंसमवेयर हमले के कारण ठप हो जाता है या किसी नागरिक का आधार से जुड़ा डेटा ऑनलाइन लीक हो जाता है, तो नुकसान केवल खोई हुई फ़ाइलों तक ही सीमित नहीं रहता - यह जनता के विश्वास को भी कम करता है। ऐसी हर घटना हमें याद दिलाती है कि गोपनीयता के बिना साइबर सुरक्षा अधूरी है, और साइबर सुरक्षा के बिना गोपनीयता असंभव है।

डिजिटल व्यक्तिगत डेटा संरक्षण (डी.पी.डी.पी) अधिनियम, 2023 देश की डिजिटल शासन यात्रा में एक महत्वपूर्ण मोड़ है। पहली बार, नागरिकों को अपने व्यक्तिगत डेटा पर लागू करने योग्य अधिकार प्राप्त हुए हैं, और संगठन इसकी सुरक्षा के लिए स्पष्ट दायित्वों से बंधे हैं। फिर भी, कानून पारित करना केवल शुरुआत है। असली चुनौती इस अधिनियम के उद्देश्य को दैनिक शासन में लागू करने में है - यह सुनिश्चित करना कि व्यक्तिगत डेटा न केवल कानूनी रूप से संसाधित हो, बल्कि उल्लंघनों, दुरुपयोग और लापरवाही से भी सुरक्षित रहे।

यहीं पर साइबर सूचना सुरक्षा शासन अपरिहार्य हो जाता है। लोगों, प्रक्रियाओं और तकनीक में संरचित जवाबदेही का निर्माण करके, यह कानूनी अनुपालन को परिचालन अनुशासन में बदल देता है। एक सुव्यवस्थित साइबर सुरक्षा ढाँचा यह सुनिश्चित करता है कि डेटा सुरक्षा किसी उल्लंघन की प्रतिक्रिया नहीं, बल्कि प्रत्येक डिजिटल प्रणाली में अंतर्निहित एक संस्कृति है।

संक्षेप में, डी.पी.डी.पी अधिनियम कानूनी आधार प्रदान करता है, लेकिन साइबर शासन इसे कार्यान्वित करने के लिए शक्ति और स्मृति प्रदान करता है। साथ मिलकर, ये दोनों मिलकर एक गोपनीयता-प्रथम, साइबर-लचीले और नागरिक-विश्वास-संचालित डिजिटल भारत की नींव रखते हैं।

सी. जे. एन्टनी
उप महानिदेशक व एचओजी
antony@nic.in

मनोज के. कुलश्रेष्ठ
वरिष्ठ तकनीकी निदेशक
mkk@nic.in

डिजिटल व्यक्तिगत डेटा संरक्षण (डी.पी.डी.पी) अधिनियम, 2023 नागरिकों के व्यक्तिगत डेटा पर अधिकार स्थापित करता है और संगठनों को इसकी सुरक्षा सुनिश्चित करने का आदेश देता है। हालाँकि, वास्तविक अनुपालन के लिए साइबर सूचना सुरक्षा शासन की आवश्यकता होती है - एक ऐसा ढाँचा जो सभी प्रणालियों, लोगों और प्रक्रियाओं में जवाबदेही, सतर्कता और अनुशासन को समाहित करता है। गोपनीयता और साइबर सुरक्षा को एक शासन मॉडल के अंतर्गत एकीकृत करके, संगठन प्रतिक्रियाशील अनुपालन से सक्रिय विश्वास निर्माण की ओर बढ़ सकते हैं। क्षेत्र-विशिष्ट मॉडल, एकीकृत निगरानी और जवाबदेही की संस्कृति इस अधिनियम को लागू करने के लिए आवश्यक हैं। अंततः, साइबर शासन डेटा सुरक्षा को एक कानूनी आवश्यकता से डिजिटल जिम्मेदारी, लचीलेपन और नागरिक विश्वास की संस्कृति में बदल देता है।

डी.पी.डी.पी के बाद साइबर गवर्नेंस क्यों मायने रखता है?

डिजिटल व्यक्तिगत डेटा संरक्षण (डी.पी.डी.पी) अधिनियम, 2023 प्रत्येक संगठन के लिए अनिवार्य करता है कि वह व्यक्तिगत डेटा की सुरक्षा के लिए "उचित सुरक्षा उपाय" अपनाए। लेकिन सरकारी प्रणालियों, स्टार्ट-अप्स और सार्वजनिक प्लेटफार्मों के जटिल डिजिटल पारिस्थितिकी तंत्र में, वास्तव में किसे उचित माना जाता है? अकेले तकनीक इस प्रश्न का उत्तर नहीं दे सकती। इसके लिए संरचना, जवाबदेही और दूरदर्शिता की आवश्यकता होती है - जो साइबर सूचना सुरक्षा शासन का मूल सार है।

साइबर शासन एक ऐसा ढाँचा प्रदान करता है जो अनुपालन को सुसंगतता में बदल देता है। यह सुनिश्चित करता है कि व्यक्तिगत डेटा की सुरक्षा व्यक्तिगत निर्णय या बाद में विचार करने पर न छोड़ी जाए, बल्कि संस्थान की योजना का हिस्सा बन जाए। खतरों पर प्रतिक्रिया करने के बजाय, शासन जाँच और संतुलन की एक सक्रिय प्रणाली बनाता है जो सुरक्षा स्थिति की निरंतर निगरानी, मूल्यांकन और सुधार करती है।

अपने मूल में, साइबर गवर्नेंस कानून और प्रौद्योगिकी को अनुशासन के माध्यम से जोड़ता है। यह साइबर सुरक्षा नियंत्रणों को डी.पी.डी.पी के गोपनीयता सिद्धांतों के साथ संरेखित करता है डेटा न्यूनीकरण और उद्देश्य सीमा से लेकर उल्लंघन सूचना और सहमति प्रबंधन तक। परिणामस्वरूप एक ऐसा पारिस्थितिकी तंत्र बनता है जहाँ प्रत्येक विभाग, विक्रेता और डिजिटल प्लेटफ़ॉर्म एक एकीकृत जवाबदेही मॉडल के तहत काम करता है।

साइबर सूचना सुरक्षा गवर्नेंस के प्रमुख आयामों में शामिल हैं:

- **प्रणालीगत अनुशासन:** स्पष्ट नीतियाँ, परिभाषित भूमिकाएँ और प्रलेखित प्रक्रियाएँ स्थापित करना ताकि तदर्थ या प्रतिक्रियात्मक सुरक्षा प्रथाओं का स्थान लिया जा सके।
- **जोखिम प्राथमिकता:** वर्गीकरण और स्तरित सुरक्षा के माध्यम से संवेदनशील डेटा श्रेणियों - जैसे स्वास्थ्य, वित्तीय, या बायोमेट्रिक जानकारी - की सुरक्षा पहले करना।
- **निरंतर सतर्कता:** यह स्वीकार करना कि उल्लंघन अपरिहार्य हैं, लेकिन जब पता लगाने, प्रतिक्रिया और रिपोर्टिंग प्रणालियों का सुशासन हो, तो क्षति को रोका जा सकता है।
- **एकीकृत अनुपालन:** साइबर सुरक्षा उपायों को सीधे डी.पी.डी.पी दायित्वों में शामिल करना जैसे सूचित सहमति सुनिश्चित करना, डेटा संग्रह को न्यूनतम करना, और समय पर उल्लंघन का खुलासा करना।

संक्षेप में, साइबर गवर्नेंस डी.पी.डी.पी अनुपालन के लिए एक संचालन प्रणाली प्रदान करता है। यह संस्थानों को ज़िम्मेदारी से कार्य करने, त्वरित प्रतिक्रिया देने और आत्मविश्वास से उबरने की क्षमता प्रदान करता है - जिससे "उचित सुरक्षा" का सिद्धांत मापनीय, लेखापरीक्षित और स्थायी विश्वास में बदल जाता है।

वास्तविक जीवन के उदाहरण

कानून इरादे ज़ाहिर करते हैं; शासन क्रियान्वयन की परीक्षा लेता है। विभिन्न क्षेत्रों में, कई वास्तविक घटनाओं ने दिखाया है कि जब साइबर सुरक्षा और गोपनीयता ढाँचे अलग-अलग काम करते हैं, तो प्रणालियाँ कितनी नाज़ुक हो जाती हैं - और जब शासन उन्हें एक साथ बाँधता है, तो वे कितनी लचीली होती हैं।

2022 में हुए एम्स रैंसमवेयर हमले को ही लीजिए। एक जटिल घुसपैठ ने अस्पताल के सर्वरों को हफ़्तों तक ठप कर दिया, जिससे लाखों मरीज़ों के रिकॉर्ड की गोपनीयता को ख़तरा पैदा हो गया। पैच प्रबंधन, नेटवर्क विभाजन और समय पर प्रतिक्रिया के अभाव ने संकट को और बढ़ा दिया। डी.पी.डी.पी व्यवस्था के तहत, ऐसी घटना से डेटा संरक्षण बोर्ड और प्रभावित नागरिकों, दोनों को अनिवार्य उल्लंघन सूचनाएँ मिल जातीं - एक ऐसा परिदृश्य जो संरचित घटना शासन, ऑफ़लाइन बैकअप और परिभाषित एस्केलेशन चैनलों की तत्काल आवश्यकता को रेखांकित करता है।

इसी तरह, कोविन डेटा एक्सपोज़र (2021-22) ने कमज़ोर एपीआई शासन के ख़तरों को उजागर किया। नाम, संपर्क नंबर और टीकाकरण की स्थिति जैसे व्यक्तिगत विवरण अनधिकृत इंटरफेस के माध्यम से सुलभ थे। सबक स्पष्ट है: एपीआई सुरक्षा और तृतीय-पक्ष निगरानी को मुख्य प्रशासनिक कार्यप्रणालियाँ बनना चाहिए, न कि तकनीकी बाद की सोच। डी.पी.डी.पी के तहत, व्यक्तिगत डेटा का अनधिकृत प्रकटीकरण प्रत्ययी कर्तव्य का उल्लंघन होगा, जिसके परिणामस्वरूप जवाबदेही और निवारण के दावे सामने आएंगे।

इसके विपरीत, डिजिलॉकर डिज़ाइन द्वारा शासन का एक सकारात्मक उदाहरण है। संग्रहीत दस्तावेज़ों को एन्क्रिप्ट करके, डेटा संग्रह को न्यूनतम करके, और नागरिकों को साझाकरण को नियंत्रित करने का अधिकार देकर, इसने पहले ही कई डी.पी.डी.पी सिद्धांतों को क्रियान्वित कर दिया है - जिनमें उद्देश्य सीमा, डेटा न्यूनतमीकरण और उपयोगकर्ता सहमति शामिल हैं। यह साबित करता है कि गोपनीयता-प्रथम संरचना तब प्राप्त की जा सकती है जब शासन डिज़ाइन का नेतृत्व करता है, न कि जब वह विनियमन का अनुसरण करता है।

वैश्विक अनुभव भी मूल्यवान संकेत प्रदान करते हैं। 2023 में, मेटा पर जीडीपीआर के तहत €1.2 बिलियन का जुर्माना लगाया गया था, क्योंकि उसने उपयोगकर्ता डेटा को पर्याप्त सुरक्षा उपायों के बिना संयुक्त राज्य अमेरिका में स्थानांतरित कर दिया था। यह मामला एक स्पष्ट अनुस्मारक है कि सीमा पार डेटा प्रशासन एक प्रक्रियात्मक औपचारिकता नहीं है - यह विश्वास की आधारशिला है। वैश्विक स्तर पर विस्तार कर रहे भारतीय संगठनों के लिए, डी.पी.डी.पी के सीमा पार स्थानांतरण प्रावधानों का अनुपालन इसी तरह की कठोरता की मांग करेगा।

ये सभी उदाहरण एक सिद्धांत पर केंद्रित हैं: साइबर प्रशासन अनुपालन को संस्कृति में बदल देता है। जहाँ प्रशासन कमजोर था, उल्लंघन संकट में बदल गए; जहाँ प्रशासन मजबूत था, विश्वास स्वाभाविक हो गया।

क्षेत्र-विशिष्ट शासन साइबर और डेटा सुरक्षा के लिए मॉडल

कोई भी दो क्षेत्र एक जैसे जोखिमों का सामना नहीं करते। मरीज़ों के रिकॉर्ड के प्रति अस्पताल की ज़िम्मेदारी, वित्तीय लेनदेन को सुरक्षित रखने के बैंक के दायित्व या ग्राहक की पहचान की सुरक्षा

▼ तालिका 11.1 **वास्तविक जीवन के उदाहरण**

मामला	शासन पाठ	डी.पी.डी.पी प्रासंगिकता / मुख्य बातें
एम्स रैनसमवेयर हमला (2022)	कमजोर पैचिंग और विलंबित प्रतिक्रिया ने अस्पताल प्रणालियों को पंगु बना दिया।	डीपीबी को उल्लंघन की अनिवार्य रिपोर्टिंग; नेटवर्क विभाजन, ऑफलाइन बैकअप और घटना प्रशासन की आवश्यकता पर प्रकाश डाला गया।
कोविन डेटा एक्सपोज़र (2021-22)	अपर्याप्त एपीआई प्रशासन के कारण अनाधिकृत डेटा तक पहुंच संभव हुई।	अनधिकृत प्रकटीकरण से प्रत्ययी कर्तव्य का उल्लंघन होता है; मजबूत एपीआई सुरक्षा और तृतीय-पक्ष ऑडिट पर जोर दिया जाता है।
डिजिलॉकर प्लेटफॉर्म	एन्क्रिप्शन, न्यूनतम डेटा संग्रहण, तथा नागरिक-नियंत्रित साझाकरण, डिजाइन द्वारा गोपनीयता सुनिश्चित करते हैं।	डी.पी.डी.पी सिद्धांतों का आदर्श उदाहरण - सहमति, उद्देश्य सीमा, और कार्रवाई में डेटा न्यूनतमीकरण।
मेटा जीडीपीआर जुर्माना (2023)	डेटा स्थानांतरण में सीमा पार सुरक्षा उपायों का अभाव।	भारतीय संस्थाओं को इसी प्रकार के दंड से बचने के लिए डी.पी.डी.पी के अंतर्गत वैध हस्तांतरण नियंत्रण लागू करना होगा।

के दूरसंचार ऑपरेटर के कर्तव्य से मौलिक रूप से भिन्न होती है। डी.पी.डी.पी अधिनियम संदर्भ-विशिष्ट सुरक्षा उपायों की माँग करके इस विविधता को स्वीकार करता है - एक सिद्धांत जो साइबर शासन के मूल में है।

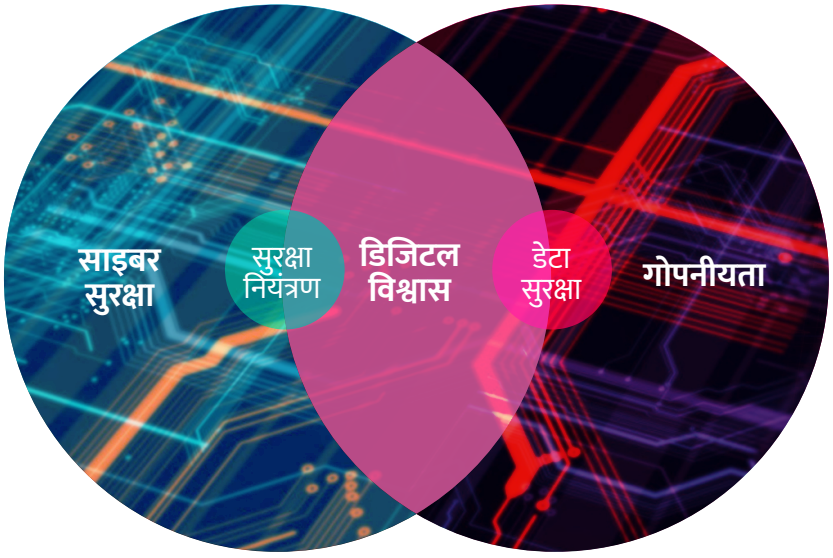
स्वास्थ्य सेवा क्षेत्र में, रैंसमवेयर और पहचान की चोरी सबसे बड़े खतरे बने हुए हैं। अस्पतालों और टेलीमेडिसिन प्रदाताओं को स्वास्थ्य संबंधी जानकारी को संवेदनशील व्यक्तिगत डेटा के रूप में वर्गीकृत करना होगा, मरीजों के रिकॉर्ड को एन्क्रिप्ट करना होगा, और नियमित रूप से गोपनीयता प्रभाव आकलन (पीआईए) करना होगा। एम्स की घटना ने दिखाया कि नेटवर्क विभाजन और अनुशासित पैचिंग के बिना, महत्वपूर्ण सार्वजनिक संस्थानों को भी लंबे समय तक व्यवधान का सामना करना पड़ सकता है।

वित्तीय क्षेत्र आरबीआई और अब डी.पी.डी.पी की दोहरी नियामक निगरानी में काम करता है। यहाँ, शासन का अर्थ है शून्य विश्वास संरचना को अपनाना, बहु-कारक प्रमाणीकरण लागू करना और समय-समय पर तनाव परीक्षण करना। 2018 में कॉसमॉस बैंक साइबर डकैती ने उजागर किया कि कैसे अनियंत्रित एंडपॉइंट और कमज़ोर विक्रेता निगरानी अच्छी तरह से विनियमित संस्थाओं को भी खतरे में डाल सकती है।

दूरसंचार और डिजिटल संचार में, ध्यान डेटा न्यूनीकरण और विक्रेता शासन पर केंद्रित होना चाहिए। दूरसंचार ऑपरेटर भारी मात्रा में व्यक्तिगत डेटा संभालते हैं - कॉल लॉग से लेकर जियोलोकेशन ट्रेल्स तक - जिससे वैध इंटरसेप्शन नीतियाँ और सीमा-पार डेटा सुरक्षा उपाय अपरिहार्य हो जाते हैं। वोडाफ़ोन यूके के जीडीपीआर जुर्माने जैसे अंतर्राष्ट्रीय मामले, कमज़ोर आंतरिक नियंत्रण और अपर्याप्त पारदर्शिता के जोखिमों को दर्शाते हैं।

सार्वजनिक क्षेत्र और ई-गवर्नेंस प्लेटफ़ॉर्म नागरिक विश्वास के केंद्र में हैं। आधार, कोविन और डिजिलॉकर जैसे प्लेटफ़ॉर्म बड़े पैमाने की डेटा प्रणालियों की कमज़ोरियों और मज़बूतियों, दोनों को प्रदर्शित करते हैं। डिज़ाइन द्वारा गोपनीयता को एकीकृत करना,

साइबर सुरक्षा + गोपनीयता = डिजिटल विश्वास



▼ तालिका 11.2 **साइबर और डेटा सुरक्षा के लिए क्षेत्र-विशिष्ट शासन मॉडल**

सेक्टर	प्रमुख जोखिम	शासन प्राथमिकता	उदाहरण/पाठ
स्वास्थ्य देखभाल	रैनसमवेयर, पहचान की चोरी, अनधिकृत अनुसंधान उपयोग	स्वास्थ्य डेटा को एन्क्रिप्ट करें, पहुंच को प्रतिबंधित करें, संवेदनशील के रूप में वर्गीकृत करें, गोपनीयता प्रभाव आकलन करें	एम्स रैनसमवेयर हमला - खंडित नेटवर्क और समय पर प्रतिक्रिया की आवश्यकता
वित्तीय सेवाएं	धोखाधड़ी, फ़िशिंग, अंदरूनी दुरुपयोग	शून्य विश्वास संरचना अपनाएं, बहु-कारक प्रमाणीकरण लागू करें, आरबीआई और डी.पी.डी.पी मानदंडों के साथ संरेखित करें	कॉसमॉस बैंक डकैती - एंडपॉइंट निगरानी और मजबूत विक्रेता निरीक्षण आवश्यक
दूरसंचार और डिजिटल संचार	सिम स्वैप, डेटा दुरुपयोग, निगरानी	विक्रेता प्रशासन को मजबूत करें, डेटा न्यूनीकरण लागू करें, वैध अवरोधन अनुपालन सुनिश्चित करें	वोडाफोन यूके जीडीपीआर जुर्माना - पारदर्शी ग्राहक डेटा के लिए शासन
ई-गवर्नेंस / सार्वजनिक क्षेत्र	एपीआई लीक, बड़े पैमाने पर डेटा एक्सपोज़र	डिज़ाइन द्वारा गोपनीयता को एकीकृत करें, निगरानी को केंद्रीकृत करें, सीईआरटी-इन रिपोर्टिंग सुनिश्चित करें	कोविन एक्सपोजर बनाम डिजिलॉकर का एन्क्रिप्शन - शासन परिपक्वता के विपरीत परिणाम
शिक्षा	बाल डेटा शोषण, प्रोफाइलिंग, पहचान की चोरी	सुरक्षित शिक्षण प्लेटफ़ॉर्म, नाबालिगों के लिए माता-पिता की सहमति, सख्त एडटेक विक्रेता ऑडिट	एडमोडो उल्लंघन - सुरक्षा की आवश्यकता दीक्षा और स्वयम् उपयोगकर्ता डेटा
महत्वपूर्ण बुनियादी ढांचा	रैनसमवेयर, तोड़फोड़, राष्ट्रीय व्यवधान	आईटी/ओटी नेटवर्क को अलग करें, एनसीआईआईपीसी फ्रेमवर्क अपनाएँ, रेड-टीम अभ्यास चलाएँ	औपनिवेशिक पाइपलाइन हमला - भारत के स्मार्ट ग्रिड लचीलेपन का मुख्य उदाहरण
एआई और उभरती हुई तकनीक स्टार्टअप्स	पुनः पहचान, पूर्वाग्रह, बिना सहमति के डेटा का उपयोग	गोपनीयता-संरक्षण एआई को लागू करें, सहमति प्राप्त डेटासेट सुनिश्चित करें, ऑडिट ट्रेल्स बनाए रखें	एआई मॉडल के दुरुपयोग के मामले - डी.पी.डी.पी के साथ संरेखित नैतिक एआई प्रशासन की आवश्यकता

सीईआरटी-इन रिपोर्टिंग सुनिश्चित करना और केंद्रीकृत शासन बोर्ड बनाना अब सभी सरकारी डेटा प्रणालियों के लिए अनिवार्य है।

शिक्षा के क्षेत्र में, छात्रों के डेटा की सुरक्षा विशेषकर नाबालिगों के लिए अभिभावकों की सहमति के ढाँचे, सुरक्षित शिक्षण प्रबंधन प्रणालियों (एलएमएस) और एडटेक सहयोगों में विक्रेताओं की कड़ी निगरानी की आवश्यकता होती है। एडमोडो उल्लंघन, जिसने लाखों छात्रों के रिकॉर्ड उजागर किए, इस बात पर प्रकाश डालता है कि भारत के दीक्षा और स्वयं प्लेटफ़ॉर्म को मज़बूत शासन स्तर क्यों विकसित करने चाहिए।

महत्वपूर्ण बुनियादी ढाँचे के लिए, जोखिम अस्तित्वगत हैं। पावर ग्रिड, परिवहन नेटवर्क और स्मार्ट सिटी सिस्टम आईटी और परिचालन तकनीक (ओटी) के मिश्रण पर निर्भर करते हैं। यहाँ शासन का अर्थ है सख्त नेटवर्क पृथक्करण, वास्तविक समय निगरानी, और एनसीआईआईपीसी ढाँचों के अनुरूप रेड-टीम अभ्यास। अमेरिका में कोलोनियल पाइपलाइन हमला एक चेतावनी के रूप में कार्य करता है: एक भी उल्लंघन पूरी राष्ट्रीय आपूर्ति श्रृंखला को बाधित कर सकता है।

अंततः, एआई और उभरती हुई प्रौद्योगिकी स्टार्टअप नए शासन के आयाम प्रस्तुत करते हैं। प्रशिक्षण डेटासेट, व्यवहार विश्लेषण और जनरेटिव मॉडल नई गोपनीयता चुनौतियाँ खड़ी करते हैं - पुनः-पहचान जोखिमों से लेकर एल्गोरिथम संबंधी पूर्वाग्रह तक। इन संस्थाओं के लिए डी.पी.डी.पी अनुपालन गोपनीयता-संरक्षण एआई तकनीकों, पारदर्शी मॉडल शासन और प्रशिक्षण प्रणालियों में डेटा के उपयोग के लिए स्पष्ट सहमति पर निर्भर करेगा।

सभी क्षेत्रों में, एक सच्चाई कायम है: शासन को अनुकूलित होना चाहिए, लेकिन जवाबदेही पूर्ण बनी रहती है।

एक गोपनीयता-जागरूक शासन मॉडल न केवल प्रणालियों की रक्षा करता है - यह नागरिकों और उनकी सेवा करने वाली संस्थाओं के बीच सामाजिक अनुबंध को भी मजबूत करता है।

डी.पी.डी.पी के बाद के युग में प्रमुख शासन क्षेत्र

डिजिटल व्यक्तिगत डेटा संरक्षण (डी.पी.डी.पी) अधिनियम, 2023 केवल एक कानून नहीं है - यह एक परिवर्तनकारी मील का पत्थर है जो हमारे देश में संगठनों द्वारा व्यक्तिगत डेटा के संचालन, प्रसंस्करण और सुरक्षा के तरीके को नया रूप देता है। यह अनुपालन-आधारित डेटा प्रबंधन से जवाबदेही-संचालित शासन की ओर एक निर्णायक बदलाव का प्रतीक है, जहाँ नागरिकों के डेटा की सुरक्षा एक रणनीतिक आवश्यकता और नैतिक दायित्व दोनों बन जाती है।

इस नए युग में, साइबर सुरक्षा को अब केवल तकनीकी या आईटी चिंता के रूप में नहीं देखा जाता। यह एक प्राथमिक प्राथमिकता बन गई है, जिसके लिए अनुपालन टीमों, वरिष्ठ प्रबंधन और व्यावसायिक नेतृत्व की सक्रिय भागीदारी आवश्यक है। यह अधिनियम संगठनों को ऐसी संरचनाएँ बनाने के लिए बाध्य करता है जो कानूनी जागरूकता, तकनीकी लचीलापन और संगठनात्मक संस्कृति का मिश्रण हों।

इस बदलाव को क्रियान्वित करने के लिए, आधुनिक शासन को छह परस्पर जुड़े क्षेत्रों पर ध्यान केंद्रित करना होगा।

ये सभी मिलकर एक गोपनीयता-प्रथम और साइबर-सुरक्षित संगठन की नींव रखते हैं, जो डेटा को एक वस्तु के रूप में नहीं, बल्कि एक साझा राष्ट्रीय संपत्ति के रूप में देखता है जिसकी देखभाल उसे सौंपी जाती है।

एकीकृत शासन ढाँचे

ऐसी दुनिया में जहाँ डेटा निर्बाध रूप से सिस्टम, विक्रेताओं और सीमाओं के बीच प्रवाहित होता है, खंडित नियंत्रण अब काम नहीं करते। संगठनों को एक एकल, एकीकृत शासन ढाँचे की आवश्यकता है जो गोपनीयता और साइबर सुरक्षा को एक मॉडल के अंतर्गत एकीकृत करे।

डेटा परिसंपत्तियों का मानचित्रण, स्वामित्व का निर्धारण, और विभागों में नीतियों का संरेखण, सीआईएसओ और डीपीओ के बीच साझा जवाबदेही सुनिश्चित करता है। एकीकृत एन्क्रिप्शन मानक, केंद्रीकृत निगरानी, और एकीकृत रिपोर्टिंग, अलग-थलग प्रथाओं का स्थान लेते हैं, जिससे संगठनों को अनुपालन से वास्तविक डेटा प्रबंधन की ओर बढ़ने में मदद मिलती है।

उल्लंघन प्रतिक्रिया और रिपोर्टिंग

डी.पी.डी.पी अधिनियम और सीईआरटी-इन के निर्देशों के तहत, उल्लंघनों की तुरंत सूचना दी जानी चाहिए - नियामकों और प्रभावित नागरिकों दोनों को। एक मज़बूत उल्लंघन प्रतिक्रिया प्रणाली के लिए स्पष्ट कार्यवाही पथ, फोरेंसिक तत्परता और पारदर्शी संचार की आवश्यकता होती है।

घटना प्रतिक्रिया को गोपनीयता दायित्वों के साथ एकीकृत करने से खतरों का पता लगाने और उन्हें नियंत्रित करने में मदद मिलती है, साथ ही जनता का विश्वास भी बना रहता है। एक डिजिटल लोकतंत्र में, कोई संगठन उल्लंघन पर कितनी तेज़ी और कितनी ईमानदारी से प्रतिक्रिया देता है, यह उसकी विश्वसनीयता को परिभाषित करता है।

विक्रेता और तृतीय-पक्ष निरीक्षण

अधिकांश आधुनिक उल्लंघन विक्रेताओं या आपूर्ति श्रृंखलाओं के माध्यम से होते हैं। डी.पी.डी.पी अधिनियम डेटा प्रभावित नागरिकों को अपने भागीदारों की चूकों के लिए ज़िम्मेदार ठहराता है, जिससे विक्रेता प्रशासन एक अनिवार्य प्राथमिकता बन जाता है।

सशक्त निरीक्षण में ऑनबोर्डिंग से पहले उचित परिश्रम, अनुबंधों में अनुपालन संबंधी प्रावधानों को शामिल करना, नियमित ऑडिट करना और विक्रेताओं की निरंतर निगरानी करना शामिल है। विक्रेताओं को जोखिम कारकों के बजाय विश्वास भागीदार बनाना संस्थागत लचीलेपन को मज़बूत करता है।

डेटा जीवनचक्र शासन

डेटा सुरक्षा केवल संग्रहण तक ही सीमित नहीं है, इसे संपूर्ण जीवनचक्र में, निर्माण से लेकर विलोपन तक, विस्तारित होना चाहिए। स्पष्ट अवधारण कार्यक्रम, उपयोग के दौरान एन्क्रिप्शन, और समाप्ति के बाद स्वचालित विलोपन, डेटा न्यूनीकरण के सिद्धांत को जीवंत बनाते हैं।

ऐसा जीवनचक्र शासन यह सुनिश्चित करता है कि संगठन केवल वही रखें जिसकी उन्हें आवश्यकता है, केवल वही संसाधित करें जो वैध है, और डेटा का जिम्मेदारी से निपटान करें - नीति को दैनिक अनुशासन में परिवर्तित करना।

सिसो सहयोग

डी.पी.डी.पी के बाद का युग साइबर सुरक्षा और गोपनीयता कार्यों के बीच घनिष्ठ सहयोग की माँग करता है। सिसो यह सुनिश्चित करता है कि डेटा की सुरक्षा कैसे की जाए; डीपीओ यह निर्धारित करता है कि इसे क्यों और कितने समय के लिए एकत्र किया जाए।

संयुक्त समीक्षा, साझा ऑडिट और समन्वित जोखिम आकलन सुरक्षा और अनुपालन लक्ष्यों को एकीकृत करने में मदद करते हैं। ये सभी मिलकर एक सुसंगत जवाबदेही ढाँचा बनाते हैं जो सुरक्षा और उद्देश्य के बीच संतुलन बनाता है।

जवाबदेही की संस्कृति

प्रौद्योगिकी प्रणालियों को सुरक्षित कर सकती है, लेकिन केवल संस्कृति ही संगठनों को सुरक्षित करती है। नियमित जागरूकता सत्र, फ़िशिंग अभ्यास और पासवर्ड स्वच्छता अभियान कर्मचारियों को अग्रिम पंक्ति के रक्षक बनाते हैं।

जब हर टीम - विक्रेताओं से लेकर नागरिकों से जुड़ी इकाइयों तक - डेटा को एक साझा ज़िम्मेदारी मानती है, तो शासन अनुपालन से संस्कृति की ओर विकसित होता है।

संक्षेप में, ये छह स्तंभ विश्वसनीय डिजिटल शासन की नींव रखते हैं। ये हमें याद दिलाते हैं कि डेटा सुरक्षा एक बार का अनुपालन कार्य नहीं है, बल्कि एक जीवंत अभ्यास है - जो गोपनीयता को एक कानूनी अनिवार्यता से एक राष्ट्रीय मूल्य में बदल देता है और एक लचीले और विश्वसनीय डिजिटल भारत का आधार बनता है।

चुनौतियाँ

डिजिटल व्यक्तिगत डेटा संरक्षण (डी.पी.डी.पी) अधिनियम, 2023 को नीति से व्यवहार में लागू करना नए नियमों का मसौदा तैयार करने से कम और संस्थाओं के व्यवहार को बदलने से ज़्यादा है। हालाँकि यह कानून दिशा प्रदान करता है, लेकिन इसके कार्यान्वयन में कई परिचालनात्मक और सांस्कृतिक बाधाएँ हैं जिनका समाधान साइबर शासन को सही मायने में स्थापित करने के लिए किया जाना चाहिए।

"उचित सुरक्षा उपायों" की परिभाषा

"उचित सुरक्षा उपायों" के लिए अधिनियम की आवश्यकता लचीलापन प्रदान करती है, लेकिन साथ ही अस्पष्टता भी। ठोस मानदंडों के बिना, व्याख्याएँ काफ़ी भिन्न हो सकती हैं - कुछ संगठन सुरक्षा में कम निवेश कर सकते हैं, जबकि अन्य अनावश्यक नियंत्रणों पर ज़्यादा खर्च कर सकते हैं।

एकरूपता लाने के लिए, संगठनों को अपने शासन को वैश्विक मानकों जैसे आईएसओ 27001 (सूचना सुरक्षा), आईएसओ 27701 (गोपनीयता सूचना प्रबंधन), या एन.आई.एस.टी. साइबर सुरक्षा ढाँचे पर आधारित करना चाहिए। सी.ई.आर.टी.-इन के निर्देशों के साथ संरेखित होने पर, ये मानक "उचित" को मापने योग्य, लेखापरीक्षा योग्य और लागू करने योग्य सुरक्षा उपायों में बदल देते हैं।

लागत और अनुपालन में संतुलन

छोटे संगठनों के लिए, अनुपालन एक महंगा प्रस्ताव लग सकता है। एन्क्रिप्शन सिस्टम लागू करना, ऑडिट करना, या डेटा अधिकारियों की नियुक्ति करना वास्तविक वित्तीय और मानवीय लागतों से जुड़ा होता है।

एक चरणबद्ध अनुपालन मॉडल एक व्यावहारिक मार्ग प्रदान करता है - उच्च-जोखिम वाले डेटा और महत्वपूर्ण कार्यों को प्राथमिकता देना। सरकार साझा सुरक्षा ढाँचे, अनुपालन टूलकिट और क्षमता-निर्माण कार्यक्रमों के माध्यम से एक महत्वपूर्ण भूमिका निभा सकती है जो गोपनीयता सुरक्षा को सभी संगठनों के लिए समावेशी और साध्य बनाते हैं, न कि केवल अच्छी तरह से संसाधन संपन्न संगठनों के लिए।

कौशल अंतर को पाटना

भारत के डेटा गवर्नेंस इकोसिस्टम में दोहरी कमी है - साइबर सुरक्षा विशेषज्ञों की जो कानून को समझते हैं और वकीलों की जो तकनीक को समझते हैं। यह कौशल अंतर विभिन्न क्षेत्रों में निरंतर अनुपालन परिपक्वता में बाधा डालता है।

इससे निपटने के लिए, एनआईसी, एमईआईटीवाई और एन.सी.आई.आई.पी.सी. को क्षमता निर्माण में निरंतर प्रयासों का नेतृत्व करना चाहिए और सिसो, डीपीओ और सरकारी अधिकारियों के लिए विशेष प्रशिक्षण मॉड्यूल तैयार करने चाहिए। विश्वविद्यालयों और प्रमाणन निकायों के साथ सार्वजनिक-निजी भागीदारी, उद्योगों में डी.पी.डी.पी अधिनियम को लागू करने में सक्षम कुशल पेशेवरों की एक स्थिर पाइपलाइन सुनिश्चित कर सकती है।

नियामक ओवरलैप का प्रबंधन

कई क्षेत्र पहले से ही कई डेटा सुरक्षा व्यवस्थाओं का अनुपालन करते हैं - आईटी अधिनियम और सीईआरटी-इन के निर्देशों से लेकर आरबीआई, आईआरडीएआई और सेबी के दिशानिर्देशों तक। डी.पी.डी.पी को जोड़ने से नियामक भ्रम या "अनुपालन थकान" पैदा होने का खतरा है।

इसका समाधान सामंजस्यपूर्ण शासन ढांचे में निहित है जो इन सभी दायित्वों को प्रतिस्पर्धी के बजाय पूरक के रूप में मानते हैं। ओवरलैप का मानचित्रण करके, संगठन रिपोर्टिंग को सुव्यवस्थित कर सकते हैं, ऑडिट को एकीकृत कर सकते हैं, और एक एकल जवाबदेही संरचना स्थापित कर सकते हैं जो सभी नियामक अपेक्षाओं को सुसंगत रूप से संरेखित करती है।

प्रारंभिक प्रवर्तन का मार्गदर्शन

डी.पी.डी.पी का कार्यान्वयन तब विकसित होगा जब डेटा संरक्षण बोर्ड अपने पहले निर्णय जारी करेगा। तब तक, अनुपालन अपेक्षाएँ अस्थिर बनी रह सकती हैं।

सबसे अच्छी रणनीति सक्रिय दस्तावेज़ीकरण है - शासन संबंधी कार्रवाइयों, जोखिम आकलन और उल्लंघन प्रतिक्रियाओं का रिकॉर्ड रखना – ताकि नियामक अनिश्चितता के बीच भी उचित परिश्रम प्रदर्शित किया जा सके।

डी.पी.डी.पी के बाद साइबर शासन एक यात्रा है, कोई चेकलिस्ट नहीं। चुनौतियाँ वास्तविक हैं, लेकिन हर एक-एक अवसर प्रदान करती है - स्पष्ट मानक निर्धारित करने, संस्थागत क्षमता को मज़बूत करने और डिजिटल प्रणालियों में जवाबदेही को गहराई से समाहित करने का। कानून अधिदेश को परिभाषित करता है; शासन उसे जीवन देता है।

अग्रिम दिशा

डिजिटल पर्सनल डेटा प्रोटेक्शन (डी.पी.डी.पी) अधिनियम, 2023 के उद्देश्य को सही मायने में सार्वजनिक विश्वास में बदलने के लिए, संगठनों को गोपनीयता और साइबर सुरक्षा को अपने शासन के डीएनए में शामिल करना होगा। अनुपालन को एक चेकलिस्ट के रूप में नहीं, बल्कि हर निर्णय को निर्देशित करने वाली मानसिकता के रूप में देखा जाना चाहिए। यह परिवर्तन एकीकृत शासन से शुरू होता है - जहाँ सीआईओ, सिसो और डीपीओ तकनीक, नीति और जवाबदेही को संरेखित करने के लिए मिलकर काम करते हैं। आईएसओ 27001 और 27701 जैसे हाइब्रिड फ्रेमवर्क द्वारा समर्थित नियमित गोपनीयता और सुरक्षा प्रभाव आकलन, जोखिमों का प्रबंधन करने और तकनीकी एवं गोपनीयता मानकों को एकीकृत करने में मदद कर सकते हैं। AI-संचालित निगरानी निरंतर सतर्कता सुनिश्चित करनी चाहिए, जबकि गोपनीयता-द्वारा-डिज़ाइन सिद्धांत सुरक्षा को सिस्टम विकास का एक अभिन्न अंग बनाते हैं। एनआईसी, सी.ई.आर.टी.-इन और क्षेत्रीय नियामकों के साथ घनिष्ठ सहयोग अनुपालन में और अधिक सामंजस्य स्थापित करेगा और संस्थागत विश्वास को मजबूत करेगा।

अंततः, डी.पी.डी.पी के बाद का युग केवल कानूनी अनुपालन के बारे में नहीं है, बल्कि नागरिकों के विश्वास का निर्माण करने के बारे में है। साइबर सुरक्षा और गोपनीयता को नियामक बोझ से डिजिटल ज़िम्मेदारी की संस्कृति में विकसित होना होगा। एक सच्चा डिजिटल राष्ट्र इस बात से परिभाषित नहीं होता कि वह कितने उपकरणों से जुड़ा है, बल्कि इस बात से परिभाषित होता है कि वह प्रत्येक जुड़े हुए नागरिक को सुरक्षा, सम्मान और विश्वास प्रदान करता है।

अधिक जानकारी के लिए संपर्क करें

सी.जे. एंटनी
उप महानिदेशक एवं मुख्य कार्यकारी अधिकारी
साइबर एवं सूचना सुरक्षा प्रशासन प्रभाग
एनआईसी मुख्यालय, ए-ब्लॉक, सीजीओ कॉम्प्लेक्स
लोधी रोड, नई दिल्ली - 110003
ईमेल: antony@nic.in, फ़ोन: 011-24305740