El cumplimiento de GDPR sigue siendo un problema para las empresas

La investigación más reciente sobre GDPR (un estudio encargado por la firma internacional de abogados McDermott Will & Emery y realizado por el Instituto Ponemon) muestra que casi el 50% de los encuestados experimentaron al menos una violación de datos personales que se requería que se informara bajo GDPR en el último año.

Hubo otros hallazgos sorprendentes en el informe Keeping Pace in the GDPR Race son:

- Una cuarta parte de los encuestados en todos los países dice que su disposición y confianza para responder a una violación de datos GDPR es muy baja.
- Solo el 18% de las organizaciones tenían una gran confianza en su capacidad para comunicar una violación de datos notificable a los reguladores dentro de las 72 horas posteriores a la toma de conciencia.
- Casi la mitad (49%) de los encuestados chinos y más de un tercio (36%) de los encuestados japoneses sujetos al RGPD aún no están familiarizados con esta regulación.

El informe señala que, aunque las empresas informan que realizan importantes inversiones en el cumplimiento, todavía existen riesgos en torno a su capacidad para prevenir, y luego también responder, a las violaciones de datos. Casi la mitad de los encuestados experimentó al menos una violación de datos personales que debía ser reportada bajo el GDPR. Menos de eso (el 39% de las empresas de EE.UU. y el 45% de las empresas de la UE) informaron de una violación de datos personales a un regulador.

A medida que el GDPR introdujo los mandatos globales de las normas de seguridad de datos, uno de los mayores problemas para muchas empresas internacionales es determinar cómo sus organizaciones cumplirán con los nuevos regulación. Debido a las diferencias en la actitud hacia la ciberseguridad y la cultura en torno a la privacidad de los datos, ciertas características demográficas y regiones de todo el mundo todavía se están adaptando a la idea del GDPR.

Otro factor que contribuye en las empresas que no cumplen con las regulaciones GDPR es su incapacidad para implementar adecuadamente el personal y los recursos establecidos por la legislación. Con más atención a la seguridad de los datos, estas empresas ahora tienen que reestructurar y contratar nuevos talentos dedicados a los objetivos de ciberseguridad de la empresa. Para las organizaciones más grandes, esto podría llevar meses y años.

Fuente: IT User