Written Information Security Plans

WHAT IS A WRITTEN INFORMATION SECURITY PLAN?

While data security laws in most jurisdictions require that companies take steps to protect personal information, in some jurisdictions, and in some industries, organizations are required to develop a written program that discusses the steps taken to identify security risks and mitigate those risks through the development of policies and procedures. The policies and procedures that a company adopts to protect personal information are referred to as a written information security plan or a "WISP."

WHAT ARE ORGANIZATIONS WORRIED ABOUT?

Organizations are concerned that if they suffer a data security breach their security program – including their WISPs – will be closely examined by regulators, plaintiffs, and/or courts. As a result, organizations want to make sure that their WISPs are sufficiently detailed and documented to satisfy statutory, regulatory, and industry standards.

WHAT DO WE DO?

We look at WISPs like a regulator looks at a WISP – with an eye toward spotting inconsistencies, errors, and facial violations of the law.

WHY BCLP?

BCLP has helped hundreds of organizations respond to data security incidents, and has defended dozens of organizations from allegations that their security program was insufficient to prevent the security incident from occurring. When we review a WISP we bring the knowledge of how such documents are viewed, and used, by regulators and plaintiffs to bear.

F-DZ/8/14/2018

11977554.1

BRYAN CAVE LEIGHTON PAISNER BCLP

OFFICES

Abu Dhabi
Atlanta
Beijing
Berlin
Boulder
Brussels
Charlotte
Chicago
Colorado Springs
Dallas
Denver
Dubai
Frankfurt
Hamburg
Hong Kong
Irvine
Jefferson City
Kansas City
London
Los Angeles
Manchester
Miami
Moscow
New York
Paris
Phoenix
San Francisco
Shanghai
Singapore
St. Louis
Tel Aviv
Washington, D.C.

bclplaw.com