

Índice General

Página

CAPÍTULO 1

EL CORPORATE COMPLIANCE EN EL SECTOR BANCARIO	15
I. Qué es el compliance penal y la importancia de las medidas y controles para evitar o minimizar los riesgos penales en banca	16
1. <i>Qué es la responsabilidad penal de la persona jurídica.....</i>	16
1.1. Introducción	16
1.2. La imputación de responsabilidad penal a la empresa	16
1.3. ¿Cómo se puede eximir la persona jurídica de dicha responsabilidad penal?	17
1.4. ¿Cuándo no se exime de responsabilidad pero sí se atenúa?	17
1.5. ¿En qué circunstancias opera la responsabilidad penal de la persona jurídica?	18
1.6. Requisitos legales para poder eximirse de responsabilidad penal la empresa	19
1.7. ¿Cómo debe ser el «modelo de organización y gestión» para prevenir delitos?	20
1.8. Las penas previstas en el Código Penal para las empresas como autoras de un delito.....	21
2. <i>Consecuencias de la comisión de delitos en el sector.....</i>	22
2.1. Planteamiento	22
2.2. ¿Qué consecuencias tienen para los empleados la comisión de estos delitos?	22

2.3.	¿Qué consecuencias tienen para los Bancos la comisión de estos delitos?	23
2.4.	¿Qué esperan los Bancos de los empleados?..	24
II.	La importancia de crear una cultura corporativa sustentada en valores éticos	25
1.	<i>Ética y compliance, conceptos distintos pero complementarios</i>	25
2.	<i>La ética como elemento clave en la función del propósito, misión y estrategia de la función de compliance.</i>	27
3.	<i>El papel del compliance officer en la creación de una cultura ética</i>	30
III.	Los riesgos penales para la banca como persona jurídica y para todos los miembros de su colectivo	32
1.	<i>Principales riesgos penales en el sector bancario</i>	32
1.1.	El riesgo de delitos de alzamiento de bienes e insolvencias punibles	32
1.2.	Blanqueo de capitales y financiación del terrorismo.....	38
1.3.	El riesgo de delito de corrupción en los negocios, cohecho y tráfico de influencias y financiación ilegal de partidos políticos	45
1.4.	Estafa.....	56
1.5.	Hacienda Pública, Seguridad Social y fraude en las subvenciones.....	62
1.6.	Delitos contra el mercado y los consumidores.....	69
2.	<i>Mapa de riesgos</i>	80
3.	<i>Análisis del mapa de riesgos</i>	81
4.	<i>Casos prácticos</i>	82
4.1.	Estafa.....	82
4.2.	Revelación de secretos, daños, secretos de empresa, propiedad intelectual	84

	<u>Página</u>
4.3. Corrupción en los negocios, cohecho, tráfico de influencias y financiación ilegal de partidos políticos	85
4.4. Delitos contra el mercado y los consumidores ..	86
4.5. El blanqueo de capitales.....	88
4.6. Delito de alzamiento de bienes.....	89
4.7. Delito contra la Hacienda Pública, Seguridad Social. El fraude en las subvenciones	90
 CAPÍTULO 2	
COMPLIANCE Y PROTECCIÓN DE DATOS EN EL SECTOR BANCARIO.....	
I. Introducción a la protección de datos	94
1. <i>El origen de la protección de datos</i>	<i>94</i>
2. <i>¿Qué es un dato personal?.....</i>	<i>96</i>
3. <i>¿Qué es un tratamiento de datos personales?.....</i>	<i>97</i>
4. <i>¿Qué es un fichero de datos personales?.....</i>	<i>98</i>
5. <i>¿Qué principios deben respetarse en el tratamiento de datos?.....</i>	<i>98</i>
6. <i>¿Cuál es el nuevo régimen sancionador?.....</i>	<i>99</i>
7. <i>Normativa aplicable en materia de protección de datos en el sector bancario</i>	<i>100</i>
8. <i>¿Qué medidas pueden adoptarse en el sector bancario?.....</i>	<i>100</i>
II. El legítimo tratamiento de los datos	101
1. <i>¿En qué consiste el legítimo tratamiento de los datos?.....</i>	<i>101</i>
1.1. <i>Porque el interesado ha prestado su consentimiento</i>	<i>101</i>
1.2. <i>Porque existe una relación contractual entre el interesado y la empresa</i>	<i>104</i>
1.3. <i>Porque existe un interés legítimo prevalente de la empresa o de terceros a los que se ceden o comunican los datos personales</i>	<i>104</i>

	<u>Página</u>
1.4. Por una necesidad vital del interesado.....	104
1.5. Por una obligación legal para la empresa	105
1.6. Por un interés público o que se derive del ejercicio de poderes públicos.....	105
2. Régimen sancionador	105
3. ¿Qué medidas pueden adoptarse en el sector bancario?.....	105
4. ¿Cómo se pronuncian nuestros tribunales?.....	106
III. Los derechos del interesado: ARCO-POL.....	108
1. ¿En qué consisten los derechos ARCO-POL?.....	108
2. Ejercicio de los derechos del interesado.....	112
3. Régimen sancionador	112
4. ¿Qué medidas pueden adoptarse en el del sector bancario?.....	112
IV. El responsable del tratamiento.....	113
1. ¿Quién es el responsable del tratamiento?.....	113
2. Obligaciones del responsable del tratamiento.....	114
2.1. Garantizar el tratamiento conforme al RGPD	114
2.2. Acreditar y demostrar el cumplimiento	114
2.3. Proteger los datos desde el diseño (Privacy by Design) y por defecto (Privacy by Default)	115
2.4. Cooperar con la autoridad de control. El sistema de «ventanilla única».....	116
2.5. Actualizar su política de protección de datos	116
2.6. Mantener un registro de actividades de tratamientos	116
2.7. Realizar una evaluación de impacto sobre la protección de datos (EIPD o PIA).....	117
2.8. Nombrar un representante de responsable de tratamiento no establecido en la Unión ...	119
2.9. Notificar las violaciones de seguridad de los datos en la empresa a la autoridad de control.....	119

	<i>Página</i>
2.10. Comunicar violaciones de seguridad de los datos al interesado	120
2.11. Nombrar un Delegado de Protección de datos (DPD o DPO)	121
2.12. Promover Códigos de conducta y esquemas de certificación.....	121
3. <i>Régimen sancionador</i>	122
4. <i>¿Qué medidas debe adoptar la empresa como responsable del tratamiento?</i>	122
V. El encargado del tratamiento	122
1. <i>¿Quién es el encargado del tratamiento?</i>	122
2. <i>Obligaciones del encargado del tratamiento</i>	123
3. <i>Régimen sancionador</i>	123
4. <i>¿Qué medidas debe adoptar la empresa respecto a la figura del encargado de tratamiento?</i>	124
VI. El delegado de protección de datos	124
1. <i>Funciones</i>	124
2. <i>Nombramiento</i>	125
3. <i>¿Qué funciones tiene el delegado de protección de datos?...</i>	128
4. <i>Régimen sancionador</i>	131
5. <i>¿Es obligatorio el nombramiento de un DPO en el sector bancario?</i>	131
VII. Ficheros de solvencia patrimonial y de crédito	131
1. <i>Introducción y encaje normativo</i>	131
2. <i>Ficheros de cumplimiento o incumplimiento de obligaciones dinerarias en España con mayor número de incidencias registradas ..</i>	135
3. <i>Requisitos de inclusión en un fichero de cumplimiento o incumplimiento de obligaciones dinerarias</i>	137
VIII. La evaluación de impacto en la protección de datos (EIPD)	145
1. <i>¿En qué consiste?</i>	145

	<u>Página</u>
2. ¿En qué casos es obligatorio realizar una evaluación de impacto?.....	146
3. ¿Cuáles son las finalidades de una evaluación de impacto?	147
4. Contenido de una EIPD o PIA.....	147
5. Procedimiento.....	148
5.1. Análisis de necesidad. Equipo de trabajo y definición del proyecto.....	149
5.2. Descripción del proyecto y de los flujos de información. Detalle de las categorías de datos que se tratan, los usuarios, los flujos de información y las tecnologías utilizadas	150
5.3. Identificación de los riesgos.....	150
5.4. Análisis de los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad de que sucedan y del daño que causarían si se materializaran. Consultas a los afectados	151
5.5. Gestión de los riesgos identificados.....	151
5.6. Análisis del cumplimiento normativo.....	151
5.7. Informe final	152
5.8. Implantación de las recomendaciones.....	152
5.9. Revisión y realimentación	152
6. Régimen sancionador	152
IX. Las transferencias internacionales de datos (TID).....	153
1. ¿Cuándo se produce una transferencia internacional de datos?.....	153
2. Requisitos en la realización de transferencias internacionales de datos.....	153
3. Suspensión temporal de las transferencias internacionales de datos	155
4. Régimen sancionador	156

	<u>Página</u>
X. La ciberseguridad	157
1. <i>Introducción</i>	157
2. <i>Los datos personales protegen a los otros activos</i>	158
3. <i>Riesgos más habituales: ciberataque, engaño, divulgación involuntaria</i>	158
3.1. Ciberataque	158
3.2. Engaño	160
3.3. Divulgación involuntaria	161
4. <i>Medidas de seguridad sobre los datos</i>	161
4.1. La seudonimización	162
4.2. La anonimización	163
4.3. El cifrado	164
4.4. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.....	164
4.5. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico ..	165
4.6. El establecimiento de un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas	165
XI. LOS DERECHOS DIGITALES	165