MICHELIN *BINDING CORPORATE RULES* (BCR) para la Transferencia de Datos de Carácter Personal desde la Unión Europea

ÍNDICE.

XX. Responsabilidad - acción disciplinaria (nota: las cláusulas 2004/915/CE son aceptables únicamente cuando un acuerdo intra-grupo ha sido firmado)

XXI. Cooperación con las autoridades de control.

XXII. Actualización de las BCR.

XXIII. Ley aplicable.

XXIV. Resolución amistosa de conflictos. Jurisdicción

XXV. Vigencia – Duración.

ANEXOS

Estas BCR incluyen los anexos siguientes:

- Anexo 1: Lista de entidades del grupo Michelin exportadoras e importadoras de Datos de Carácter Personal.

- Anexo 2: Operaciones de tratamiento regidas por las presentes BCR.

- Anexo 3: Descripción del cometido de los “Privacy Officers” y de la misión del Comité de privacidad.

- Anexo 4: Nota informativa sobre los procedimientos internos del grupo Michelin, procedimientos del grupo, y nota de presentación, y proceso de auditoría interna de Michelin.

- Anexo 5: Programa de verificación del cumplimiento de las BCR.

- Anexo 6: Guía del usuario.

I. OBSERVACIONES PRELIMINARES.

De conformidad con la Directiva Europea 95/46/CE de 24 de octubre de 1995, y la Directiva 02/58/EC de la Unión Europea de fecha 12 de julio de 2002, estas *Binding Corporate Rules* tienen por objeto proporcionar garantías suficientes para que los datos personales, en particular, los de los empleados, clientes y proveedores del grupo Michelin, queden protegidos en cualquier transferencia de los mismos que realicen las entidades del grupo Michelin con sede en un Estado miembro de la UE, o en un país que garantice un nivel adecuado de protección, a otras entidades del grupo Michelin con sede en otros países (fuera de la UE) que no garanticen un nivel adecuado de protección.

II. DEFINICIONES.

Las definiciones sobre Datos de Carácter Personal, Tratamiento de Datos de Carácter Personal, así como las de Responsable y Encargado contenidas en estas BCR, son las detalladas en la Directiva 95/46/CE de 24 de octubre de 1995.

Los términos y expresiones utilizadas en estas BCR tienen el siguiente significado:

"Datos Personales", "Datos" toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

"Datos sensibles", toda información de una persona relativa al origen racial o étnico, político, ideológico, filosófico o religioso, afiliación sindical, la salud o la orientación sexual.

"Entidad", cualquier entidad jurídica del grupo Michelin que exporte o importe datos de Carácter Personal.

"Exportador de datos personales o exportador", sociedad del grupo de Michelin, con sede en la Unión Europea o en un país que garantiza un nivel adecuado de protección, que transfiere datos personales a otra entidad del grupo Michelin, con sede en un país que no garantiza un nivel adecuado de protección.
"Finalidad del tratamiento", objetivo (s) de una aplicación, finalidad en virtud de la cual los datos de carácter personal, cualquiera que sea el medio utilizado (electrónico, papel u otros) que posibilite el tratamiento de dichos datos.

"Importador de datos personales o Importador", entidad del grupo Michelin, con sede en un país fuera de la UE, que no garantiza un nivel adecuado de protección, que recibe datos de carácter personal de un Exportador o/y de otro Importador, procesados dentro de la Unión Europea.

"País que garantiza un nivel adecuado de protección", 1) los Estados miembros de la UE, y; 2) Liechtenstein, Noruega e Islandia, 3) los países para los que la Comisión Europea ha

emitido una decisión afirmativa sobre su nivel adecuado de protección: Canadá, Argentina, Suiza, Isla de Man, Guernsey, y/o 4) todos los países que puedan adherirse a la Unión Europea y/o sobre los que se tome una decisión positiva sobre su adecuada protección.

"Interesado", persona física identificada o identificable titular de los datos que son objeto del tratamiento o de la transferencia.

"Oficial de Privacidad" "Privacy officer", persona física a cargo de la protección de datos personales de cada empresa del grupo Michelin.

"Responsable del Tratamiento de los datos" (Exportador o Importador)", la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario. Dentro del grupo Michelin, el Responsable de los datos es la persona jurídica representada por el empleado, ya sea Jefe de Departamento o no, que determina los fines y los medios de procesamiento.

"Encargado del Tratamiento de los Datos", la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

"Tratamiento de los Datos de Carácter Personal", "Tratamiento", cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

"Transferencia", cualquier revelación/divulgación de datos personales a través de una red o cualquier revelación/divulgación de un medio a otro, independientemente del tipo de medio, en la medida en que tales datos son destinados al tratamiento en el país receptor, excepto en situaciones en las que los datos simplemente cruzan el territorio de la Unión Europea.

III. Responsable de aplicar las BCR.

La compañía matriz del grupo Michelin, *Compagnie Générale des Etablissements Michelin*, que se constituye y rige por la legislación francesa, debido a su papel central en la organización operativa del grupo Michelin, ha delegado en la sociedad del grupo *Manufacture Française des Pneumatiques Michelin* (en lo sucesivo, MFPM), igualmente constituida y regida por la legislación francesa, la responsabilidad de aplicar las normas BCR para la protección de datos personales dentro del grupo Michelin durante cualquier transferencia de datos personales de la Unión Europea.

IV. Sociedades del grupo Michelin en las que BCR resultan aplicables.

El propósito de estas BCR es organizar los flujos transfronterizos de datos personales entre los Exportadores y los Importadores que figuran en el Anexo 1.

Los Exportadores e Importadores se comprometen a cumplir las presentes BCR. Se ha elaborado una directiva del grupo y un sistema de gestión de grupos organizados a través de la creación de un Comité de Protección de datos personales, presidido por el Director del Departamento Jurídico del grupo, quien también es responsable de la protección mundial de Datos de Carácter Personal. Así mismo, este Comité está compuesto por los directores de los departamentos de recursos humanos, sistemas y servicios de seguridad del grupo.

V. Descripción de las operaciones de tratamiento.

Las presentes BCR se refieren a las operaciones de procesamiento, ya sea automatizada o no, especificado en el Apéndice 2, que incluyen datos de carácter personal que han sido procesados en la Unión Europea y trasladados fuera de la Unión Europea para su procesamiento.

VI. Requisitos particulares respecto de las entidades del grupo.

Cada Exportador y/o Importador debe garantizar y asegurar que las operaciones de tratamiento de datos personales cumplen con la legislación local y con las presentes BCR.

VII. Obligaciones del Exportador de datos como Responsable de los datos.

Los Exportadores deben cumplir con la ley nacional aplicable en el Estado miembro correspondiente de la Unión Europea en el tratamiento y la transferencia de los datos que están a su cargo.

Los Exportadores garantizan que han realizado una declaración a la autoridad nacional de control correspondiente del tratamiento previsto o que han obtenido, como podría ser el caso, la autorización requerida para realizar estos tratamientos, y que el tratamiento que han efectuado, incluida la transferencia prevista, ha sido es y será realizado cumpliendo con las presentes BCR.

Siempre que se cumplan las disposiciones nacionales adoptadas en virtud de la Directiva Comunitaria 95/46/CE, de 24 de octubre de 1995, el Exportador puede, así mismo, transferir datos personales a un tercer país que no garantice un nivel adecuado de protección, siempre que:

- El Interesado haya dado su consentimiento inequívoco para la realización de la transferencia.
- La transferencia fuera necesaria por una de las siguientes razones:

1. Para proteger el interés vital del interesado.
2. Para llevar a cabo una misión de interés público.
3. Para establecer, ejercer o defender una reclamación legal.
4. Consultar, en condiciones normales, un registro que, de acuerdo con las leyes o reglamentos, está destinado a proporcionar información al público y que está disponible para

ser consultado por el público en general o por cualquier persona que pueda demostrar un interés legítimo.
5. Para celebrar un contrato entre el Interesado y el Responsable del tratamiento, o implementar medidas pre-contractuales adoptadas en respuesta a la solicitud del interesado.
6. Concluir o celebrar un contrato en interés del Interesado entre el Responsable y un tercero.

7.1 Normas relativas al tratamiento de datos personales.

Siempre que se cumplan las disposiciones nacionales adoptadas en virtud de la Directiva 95/46/CE de 24 de octubre 1995U, el tratamiento de datos personales sólo podrá efectuarse si:

- El interesado ha dado inequívocamente su consentimiento.
- El tratamiento es necesario para el cumplimiento de un contrato en el que el interesado es parte o para tomar medidas, a petición del interesado, antes de celebrar un contrato.
- Es necesario para el cumplimiento de una obligación jurídica a la que el Responsable de datos está sujeto.
- El tratamiento es necesario para salvaguardar el interés vital del interesado.
- El tratamiento es necesario para el desempeño de una misión de interés público o inherente al ejercicio del poder público conferido al Responsable de datos o a un tercero a quien se comuniquen los datos.
- El tratamiento es necesario para la satisfacción del interés legítimo perseguido por el Responsable del mismo o por un tercero o terceros a los que se comuniquen los datos, excepto cuando sobre tales intereses no prevalezcan otros concernientes a derechos fundamentales y libertades del Interesado que requieran protección en virtud del artículo 1 de la Directiva 95/46/CE, de 24 de octubre de 1995.

7.2 Normas relativas a la calidad de los datos recogidos.

Los Exportadores se comprometen a garantizar que los datos personales transmitidos a los Importadores son:

- Recogidos y tratados de manera justificada y legal.
- Recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines.
- Adecuados, pertinentes y no excesivos en relación con los fines para los que se recopilen y se traten posteriormente.
- Exactos, completos y, cuando sea necesario, actualizados.
- Conservados en una forma que permite a los Interesados ser identificados durante el tiempo estrictamente necesario para los fines para los que fueron recogidos y tratados.

7.3 Limitación de las transferencias de datos a un propósito específico.

En el marco de la transferencia de datos personales a los Importadores, los Exportadores garantizan que:

- La transferencia de datos de carácter personal se lleva a cabo para un fin específico, explícito y legítimo;
- Los datos transferidos no serán tratados de una manera incompatible con dichos fines.

7.4 Reglas para los datos sensibles.

Siempre que se cumplan las disposiciones nacionales adoptadas en virtud de la Directiva 95/46/CE de la Unión Europea, de 24 de octubre de 1995, el tratamiento de operaciones relacionadas con datos sensibles estará prohibido, salvo si:

- El interesado ha dado su consentimiento explícito a su transferencia.
- El tratamiento es necesario para los fines del cumplimiento de las obligaciones y derechos específicos del Responsable del tratamiento en materia de Derecho laboral.
- El tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.
- El tratamiento se refiere a los datos sensibles que se han hecho manifiestamente públicos por el Interesado o sea necesario para el reconocimiento, ejercicio o defensa de un derecho legal.

7.5 Normas para el cumplimiento de los compromisos del importador.

Los Exportadores garantizan haber realizado los esfuerzos razonables para asegurar que el Importador sea capaz de satisfacer las obligaciones establecidas en el Artículo VIII siguiente.

VIII. Obligaciones del Importador de datos como Responsable de los Datos.

El Importador podrá tratar y transferir datos sensibles y no sensibles a otro Importador, si las condiciones establecidas en el Artículo VII se cumplen.

Los Importadores se comprometen a que los datos transferidos de conformidad con los fines previstos en el momento de la recogida y, en consecuencia, a tratar los datos personales de una manera compatible con la finalidad de la transferencia y de conformidad con los principios establecidos para el tratamiento datos personales contenidos en los artículos VII, IX, X, XI, XII, XIII, XIV, XV y XXI de las presentes BCR.

Así mismo, los Importadores se comprometen a que los Interesados puedan ejercitar en cualquier momento los derechos reconocidos en los artículos XIX, XX siguientes.

IX. Información y derechos de los Interesados.

En los supuestos de transferencias de datos personales a un Importador, los Interesados tienen derecho a:

- Obtener, en un plazo de tiempo razonable, una copia de las presentes BCR de las personas o servicios mencionados en el Anexo 3.

- Ser informados de la transferencia de sus datos personales, el propósito de la misma, el país en el que el Importador de datos se encuentra y, en su caso, si el nivel de protección de dicho país es acorde o no con las disposiciones nacionales o de la UE (tal y como se especifica en la Directiva Europea 95/46/CE, de 24 de octubre de 1995). Los “Privacy Officers” deben ser capaces de proporcionar a los Responsables dicha información previa en relación con los empleados, proveedores, clientes y, en general, con todas las personas cuyos datos personales están ubicados en archivos de Michelin.

- Obtener el acceso a la información de sus datos sometidos a tratamiento y, en su caso, obtener su rectificación, cancelación y oposición, cuando considere que no han sido tratados de acuerdo con los principios establecidos en las presentes BCR.

- Oponerse al tratamiento de sus datos personales por motivos legítimos y justificados a su situación particular.

- Remitir el asunto a las personas o servicios mencionados en el Anexo 3 para la tramitación de sus reclamaciones o quejas.

- Remitir el asunto a la autoridad de protección de datos correspondiente.

- Remitir el asunto a los órganos jurisdiccionales competentes.

- Oponerse, de forma gratuita, al tratamiento de sus datos de carácter personal para los que el Responsable prevea un tratamiento destinado al *marketing* directo, o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en su nombre a efectos de *marketing* directo, y ofrecerle expresamente, de forma gratuita, su derecho de oposición para tales comunicaciones o usos.

X. Garantía de aplicación.

Las entidades del grupo Michelin se comprometen a adoptar todas las medidas necesarias para aplicar las presentes BCR.

XI. Formación y sensibilización.

Las entidades del grupo Michelin se comprometen a impartir programas de formación a sus empleados sobre la protección de datos personales y, en particular y sobre todo, a aquéllos que tienen acceso a dichos datos, aquéllas personas involucradas en el desarrollo de los sistemas de tratamiento, personal directivo y personal de recursos humanos, TI, auditoría y seguridad de los servicios. En Anexo 6 se muestra un ejemplo de un manual del usuario.

Igualmente, estarán disponibles para los empleados en la Intranet del grupo información relevante y actualizada sobre la transferencia de datos personales, así como una copia de las BCR: esta información también se transmitirá a través de los memorandos internos y se publicará en los tablones de anuncios para este propósito. Para los clientes y proveedores de las entidades, las presentes BCR estarán igualmente disponibles en la página Web corporativa de Michelin.

Podrán ser impuestas sanciones disciplinarias en respuesta a violaciones de los preceptos contenidos en la BCR. Estas vienen detalladas Artículo XVIII.

XII. Dificultad para las Entidades del grupo en la aplicación de las BCR.

Si un Importador tiene motivos para creer que la legislación aplicable puede impedir el cumplimiento de sus obligaciones establecidas en las BCR lo que provocaría un efecto

perjudicial sobre las garantías ofrecidas, el Importador deberá informar inmediatamente a MFPM, salvo cuando una autoridad judicial prohíba hacerlo.

En tales circunstancias, MFPM deberá adoptar una decisión de gestión y consultará a las correspondientes autoridades de protección de datos.

XIII. Restricciones sobre transferencias fuera del grupo y fuera de la Unión.

Las Entidades situadas en el origen de la transferencia fuera del grupo y fuera de la Unión Europea, se comprometen a obtener el consentimiento previo de los Interesados y a informarles de que, después de la transferencia, los datos podrán ser tratados por un Responsable del tratamiento que no esté vinculado por las presentes BCR, y que no esté establecido en un país que garantice un nivel adecuado de protección.

Antes de cualquier transferencia fuera del Grupo y/o fuera de la Unión Europea, el Interesado debe haber sido informado de lo siguiente:

- Con carácter previo, sobre el objetivo de la transferencia fuera del Grupo y fuera de la Unión Europea.
- Identificación del Exportador desde donde vienen los datos.
- Las categorías de los posteriores receptores de datos y los países receptores.

Se distinguen dos situaciones:

1. Transferencia de datos a los Responsables no pertenecientes al grupo Michelin.

Para todas las transferencias fuera del grupo y fuera de la Unión Europea, cada Importador / Exportador se compromete a celebrar un contrato con los Responsables sobre la base de las cláusulas contractuales tipo adoptadas por la Comisión Europea en su Decisión N º 2001/497/ CE, de 15 de junio de 2001, modificada el 27 de diciembre de 2004 (para las transferencias a Responsables del tratamiento), de conformidad con la Directiva 95/46/CE de 24 de octubre de 1995.

2. Transferencia de datos a los Encargados no pertenecientes al grupo Michelin.

Para todas las transferencias fuera del grupo y fuera de la Unión Europea a los Encargados, cada Importador/Exportador se compromete a celebrar un contrato con los referidos Encargados con sede en países fuera de la UE, sobre la base de las cláusulas contractuales tipo adoptadas por la Comisión Europea en su Decisión N º 2002/16/CE de 27 de diciembre de 2001 (relativo a las transferencias a los procesadores de datos), de conformidad con la Directiva 95/46/CE de 24 de octubre de 1995.

XIV. Confidencialidad.

Sólo las personas expresamente designadas para recibir la comunicación de datos podrán tener acceso a los datos de carácter personal contenidos en un archivo.

Así, a las personas designadas les está prohibido el uso de dichos datos para fines personales, la transmisión de los mismos a terceros no designados expresamente, o su uso de cualquier forma.

XV. Seguridad de los Datos.

Los Exportadores e Importadores adoptarán las medidas de seguridad de índole técnica y organizativa adecuadas y necesarias, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural, que garanticen la seguridad de los datos de carácter personal a los que acceda al objeto de evitar su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas se aplicarán a:

- La protección física y medioambiental de los IT cuartos, *hardwares* o soportes informáticos utilizados para los datos con el fin de garantizar y asegurar la continuidad del tratamiento o evitar la pérdida de información ya sea por robo o deterioro debido a incendios, daños por agua u otros desastres naturales.

- La utilización de dispositivos de seguridad (*software o hardware*) y a la administración de los derechos de acceso que proporcionan protección lógica sobre el tratamiento de datos, evitando que personas no autorizadas puedan acceder a los mismos, o que a través de un error humano dañen la integridad, disponibilidad y confidencialidad de los datos.

- Las redes de la compañía para que mediante el uso de cortafuegos y *software anti-malware* estén protegidas contra los ataques cibernéticos.

- Los datos personales transmitidos de forma segura fuera de las redes de la empresa según las instrucciones del Responsable.

- La gestión de cambios para que la continuidad, integridad, confidencialidad y seguridad de los datos estén garantizadas.

- La organización con distribución y diferenciación de funciones entre varias personas u organizaciones.

XVI. Decisiones individuales automatizadas.

Toda persona tiene derecho a no ser objeto de una decisión que entrañe efectos jurídicos sobre ella, o que le afecte de manera significativa, basada únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, solvencia, fiabilidad, conducta, etc.
Sin embargo, una persona puede quedar sometida a una decisión de ese tipo cuando dicha decisión:

a) se tome en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del mismo, propuesta por el Interesado, se haya satisfecho o que existan medidas apropiadas para la salvaguarda de sus legítimos intereses, tales como la posibilidad establecer acuerdos que le permitan defender su punto de vista.

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

XVII. Relaciones con los Encargados miembros del grupo situados dentro y fuera de la UE (Importadores) y los Encargados no pertenecientes al grupo localizados dentro de la UE.

Estas BCR cubren las transferencias de datos personales a Encargados miembros del grupo fuera de la Unión Europea, así como a Encargados no pertenecientes al mismo situados en la Unión Europea. Se trata simplemente de señalar que los Exportadores e Importadores se comprometen a poner en práctica procedimientos para garantizar que dicho Encargado cumpla con la confidencialidad y seguridad de los datos a los que se les da acceso. Los Encargados, por su parte, deben proporcionar a los Exportadores e Importadores las suficientes garantías para que la seguridad prescrita y las medidas de confidencialidad se apliquen efectivamente. Para formalizar este aspecto, los contratos celebrados entre el Responsable del tratamiento y el Encargado deberán establecer las obligaciones que recaen sobre el Encargado en materia de seguridad y confidencialidad de datos, así como igualmente deben especificar que el Encargado del tratamiento sólo deberá actuar siguiendo las instrucciones del Responsable del tratamiento.

Tras la terminación del contrato, el Encargado deberá proceder a la destrucción o, en su caso, según las instrucciones que al respecto reciba, devolución de los datos de carácter personal y de los soportes o documentos en que conste algún dato que provenga del fichero de datos correspondiente, sin conservar copia alguna del mismo y sin que ninguna persona, física ni jurídica, entre en conocimiento de tales datos.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso, deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación. Deberá igualmente garantizar que la confidencialidad de los datos está protegida y que no experimentan ninguna transformación ulterior.

XVIII. Seguimiento de la aplicación de las BCR.

Los Exportadores e Importadores han designado dentro de las entidades el llamado "Privacy Officers", quien también podrá ser designado por la correspondiente autoridad de protección de datos si así lo permitiera la legislación local. Los "Privacy Officers" son responsables de garantizar que los Responsables del tratamiento de datos cumplan con las BCR, y serán así mismo responsables de sus cometidos con la MFPM.

Los "Privacy Officers" deben llevar a cabo auditorías periódicas para garantizar que los principios establecidos en las BCR son efectivamente aplicados. Estas auditorías tienen como objetivo la fiabilidad de los controles de primer nivel llevados a cabo por los Responsables del tratamiento de conformidad con los procedimientos específico internos del grupo de Michelin que figuran en el Anexo 4, basados en el programa de verificación del cumplimiento de estas BCR que se contiene en el Anexo 5.

Una vez finalizado el procedimiento de verificación del cumplimiento referido, será elaborado y enviado un informe al administrador de privacidad global.

A petición de la autoridad de protección de datos correspondiente, podrá ser enviada a la misma una copia del informe referido.

Aproximadamente cada 5 años, el servicio de auditoría del grupo Michelin evaluará el cumplimiento de estas BCR realizadas por "Privacy Officers" con el fin de asegurar que los riesgos se gestionan. Los informes del servicio de auditoría del grupo se transmitirán al Gerente de Riesgos responsable de la ejecución de planes de gestión y las medidas correctivas del grupo, así como a la comisión ejecutiva del grupo.

XIX. Gestión de las reclamaciones.

1. En caso de litigio, los Interesados podrán presentar una reclamación por la realización de tratamientos ilegales o manipulación de sus datos personales de forma incompatible con las BCR presentes, al "Privacy Officer" de su país ya sea directamente o por carta. Sin perjuicio de las dificultades que se puedan encontrar a la hora de obtener información necesaria al respecto, las quejas deben ser investigadas dentro de un mes de su presentación.

2. En el marco de estas BCR, los "Privacy Officers" son responsables de:

- La identificación y registro de las denuncias individuales de los Interesados.
- Elaboración de una lista de esas denuncias.
- Llevar a cabo una investigación sobre la realidad de los hechos alegados y sobre la imputabilidad del hecho causante de los daños.
- Tratar de mediar ofreciendo una compensación, tras informar a MFPM. Los asuntos pueden ser remitidos a los Juzgados y/o Tribunales competentes o a la autoridad de control correspondiente después de haber sido objeto de un procedimiento de mediación y conciliación.

3. El hecho de que el tratamiento de quejas esté centralizado en la gestión de los "Privacy Officers", no puede impedir ni limitar los derechos de los Interesados en lo relativo a la presentación de sus reclamaciones ante la autoridad de protección de datos y/u órgano jurisdiccional competentes.

4. Los Interesados que hayan sufrido daños y perjuicios causados por un Importador en relación con los datos personales transmitidos por un Exportador con sede en la Unión Europea a un Importador situado en un país fuera de la UE, que la Comisión Europea no reconoce un nivel adecuado de protección, a causa de tratamientos ilícitos de o cualquier otra acción incompatible con estas BCR, tienen derecho a obtener:

- La corrección de las operaciones realizadas vulnerando las presentes BCR.
- Una indemnización por la pérdida sufrida.

5. En el marco de sus funciones, los "Privacy Officers" garantizan su independencia y están obligados a un estricto deber de neutralidad en los asuntos que están a su cargo.

XX. Responsabilidad. Acción disciplinaria.

En caso de que el Importador actúe como Encargado, el Interesado tiene derecho a obtener del Exportador una indemnización por los daños y perjuicios sufridos a causa del incumplimiento de estas BCR.

En el caso de que el Importador actúe como Responsable, Exportador e Importador de datos responden frente los Interesados por la falta de cumplimiento de sus obligaciones respectivas, tales como las que resultan de las disposiciones de las BCR, así como también responden por

los daños y perjuicios que les causen (a los Interesados) por infracción de derechos de terceros sobre la base de los artículos XVIII y XIX referidos anteriormente. Podrán ser parcial o totalmente exonerados si demuestran que la causa de este incumplimiento no es imputable a ellos.

Cada Exportador y/o Importador acepta que el Interesado tenga derecho a una indemnización por los daños y perjuicios causados por incumplimiento de estas BCR cometido un Importador en relación con los datos personales transmitidos por un Exportador, y así mismo aceptan la jurisdicción del país en el que el Exportador está localizado.

En los supuestos de reclamaciones que aleguen un incumplimiento de las obligaciones del Importador, el Interesado deberá previamente solicitar al Exportador la adopción de medidas necesarias para hacer valer sus derechos frente al Importador. Si el Exportador no tomara en un tiempo razonable medida alguna (normalmente un mes), el Interesado podrá hacer valer sus derechos directamente contra el Importador. El interesado también tiene derecho a interponer una reclamación o demanda directamente contra un Exportador que no haya tomado las medidas razonables para determinar si el Importador es capaz de satisfacer sus obligaciones bajo estas BCR.

En cualquier caso, el demandado deberá demostrar que las BCR no han sido infringidas o que el hecho causante del daño no es imputable al Importador /Exportador, siempre que la persona involucrada demuestre que ha sufrido daños y perjuicios y pruebe que el daño ha sido originado como resultado probable de un incumplimiento de las BCR.

Los Exportadores e Exportadores disponen de suficientes recursos financieros a su disposición para cubrir el pago de una indemnización por incumplimiento de las BCR.

MFPM puede igualmente adoptar medidas disciplinarias, en particular en el caso de:

- El incumplimiento de las disposiciones de las presentes BCR.
- La no aplicación de las recomendaciones y el asesoramiento recibidos a raíz de la auditoría llevada a cabo por los “Privacy Officers”
- Falta de cooperación en el marco de la autoría de cumplimiento de las BCR llevada a cabo por los “Privacy Officers”, así como con las autoridades encargadas de la protección de datos personales.

De conformidad con la legislación laboral vigente, las normas internas de empresa y con el contrato de trabajo, podrán ser adoptadas medidas disciplinarias (sanciones) contra cualquier persona que infrinja las disposiciones de las presentes BCR.

A petición de los miembros del Comité de Protección de Datos del grupo, dichas sanciones pueden incluir también las siguientes medidas:

- Publicación de las recomendaciones del “Privacy Officers” en la Intranet del Grupo.
- La publicación de las sanciones impuestas por la autoridad responsable de la protección de datos.
- La prohibición permanente o temporal de continuar con la circulación de datos.

XXI. Cooperación con las Autoridades de control.

Los Exportadores e Importadores están de acuerdo en cooperar con las autoridades de protección de datos pertinentes respondiendo dentro de un plazo razonable a todas las peticiones que les puedan hacer.

Los Exportadores e Importadores están igualmente conformes en la realización de auditorías por las autoridades de protección de datos, si fueran necesarias.

Los Exportadores e Importadores presentarán una copia de estas BCR a las autoridades de control pertinentes, si así lo requiriera la ley nacional del Estado donde el Exportador está situado.

Los Exportadores e Importadores se comprometen a seguir los consejos y recomendaciones de las autoridades pertinentes relativas a la interpretación y aplicación de estas BCR.

XXII. Actualización de las BCR.

22.1 Actualización del contenido de las BCR.

Las BCR podrán ser modificadas previa decisión del Comité de Protección de Datos Personales del grupo.

Como parte del grupo Michelin, se compromete, de acuerdo con el Artículo XXI anterior, a notificar una vez al año a las autoridades correspondientes de protección de datos, los cambios sustanciales sufridos en las BCR o en la lista de entidades del grupo Michelin, con una breve explicación de los motivos que justifican la actualización, ,

Estos cambios se pondrán a disposición de todas las Entidades, miembros del grupo Michelin.

22.2 Actualización de la lista de entidades a las que son de aplicación las BCR.

El Comité de Protección de Datos Personales se compromete a designar a una persona o departamento que se encargará de la elaboración y actualización de una lista que incluya las entidades del grupo Michelin a las que resulta de aplicación las BCR.

No podrán transferirse datos a una nueva entidad con sede en un país fuera de la UE que no garantice un nivel adecuado de protección, hasta que la entidad del grupo Michelin exportadora de los datos no se asegure de que la nueva destinataria de los datos se obligue y comprometa a cumplir las presentes BCR.

Cualquier cambio en la lista de las Entidades deberán ser notificada a las autoridades de protección de datos correspondiente.

XXIII. Ley aplicable.

Las disposiciones de las BCR se rigen por la legislación del Estado miembro de la UE en el que el Exportador se localice.

XXIV. Resolución amistosa de conflictos. Jurisdicción.

A falta de un acuerdo entre el Interesado y la Entidad del grupo Michelin o, en su defecto sin acuerdo amistoso alcanzado en el marco del procedimiento de mediación previsto en el Artículo XIX, la competencia para la resolución de los conflictos se atribuye a los Juzgados y Tribunales de la Entidad de Exportadora.

XXV. Vigencia.

Estas normas de obligado cumplimiento empresarial en vigor en la fecha de la directiva de grupo, por una duración indeterminada.

ANEXOS

Estas BCR incluyen los anexos siguientes:

- Anexo 1: Lista de entidades del grupo Michelin exportadoras e importadoras de Datos de Carácter Personal.

- Anexo 2: Operaciones de tratamiento regidas por las presentes normas corporativas vinculantes.

- Anexo 3: Descripción del cometido de los “Privacy Officers” y de la misión del Comité de privacidad.

- Anexo 4: Nota informativa sobre los procedimientos internos del grupo Michelin, procedimientos del grupo, y nota de presentación, y proceso de auditoría interna de Michelin.

- Anexo 5: Programa de verificación del cumplimiento de las BCR.

- Anexo 6: Guía del usuario.

ANEXO 1

Lista de Sociedades Exportadoras

Razón Social	País
EUROMASTER GmbH	Allemagne
EUROMASTER Immobilien GmbH	Allemagne
EUROMASTER Reifenservice Deutschland GmbH	Allemagne
Kleber Reifen GmbH	Allemagne
Korso Industriebeteiligungsgesellschaft mbH	Allemagne
Laurent Reifen GmbH	Allemagne
Leukos Handelsgesellschaft für Kautschukprodukte mbH	Allemagne
MC Syncro Supply GmbH	Allemagne
Michelin Development GmbH	Allemagne
Michelin Finanz Gesellschaft für Beteiligungen AG & Co. OHG	Allemagne
Michelin Reifenwerke AG & Co. Kommanditgesellschaft auf Aktien	Allemagne
Radsystem GmbH	Allemagne
Universal Versicherungsvermittlung Gesellschaft mit beschränkter Haftung	Allemagne
ViaMichelin Deutschland GmbH	Allemagne
Euromaster Reifenservice GmbH	Autriche
Michelin Reifenverkaufsgesellschaft m.b.H.	Autriche
Euro-Fitting Invoicing N.V.	Belgique
Euro-Fitting Management N.V.	Belgique
MCSyncro N.V.	Belgique
Michelin Belux S.A. ou N.V.	Belgique
Société pour le Traitement de l'Information TRINFOVER	Belgique
Euromaster Danmark A/S	Danemark
Euromaster DK Holding A/S	Danemark
Laurent Daek A/S	Danemark
Michelin Gummi Compagni A/S	Danemark
Euromaster Ejendomme A/S	Danemark
Viborg Direct A/S	Danemark
Ensamblaje y Logística de Conjuntos, S.A.	Espagne
EUROMASTER AUTOMOCIÓN Y SERVICIOS, S.A.	Espagne
Fundación Michelin Desarrollo	Espagne
MCSyncro Vigo, S.A.	Espagne
Michelin España Portugal, S.A.	Espagne
ViaMichelin España, S.L.	Espagne
Michelin Rehvide AS	Estonie
Oy Suomen Michelin Ab	Finlande
Suomen Euromaster Oy	Finlande
Adaran	France
Compagnie Générale des Etablissements Michelin	France
Euromaster France	France

Razón Social	País
Euromaster Services et Management	France
Jean Estager et Cie	France
Manufacture Française des Pneumatiques Michelin	France
MCSyncro France	France
Michelin Air Services	France
Michelin Aircraft Tyre	France
MICHELIN FACILITIES EUROPE	France
Michelin Middle East	France
Pneu Laurent	France
Pneumatiques Kléber	France
RADSYSTEM HAMBACH	France
Recamic Services	France
S.CI. DE VITOT	France
S.O.D.G.	France
Simorep et Cie - Société du Caoutchouc Synthétique Michelin	France
SOCIETE CIVILE IMMOBILIERE DE LA MONTAT	France
SOCIETE CIVILE IMMOBILIERE DU CHALET	France
Société Civile Immobilière Michelin Breteuil	France
SOCIETE CIVILE LANGUEDOC PLAISANCE	France
Société de Développement Mécanique	France
Société de Technologie Michelin	France
Société des Procédés Industriels Modernes	France
Société d'Etudes et d'Applications Michelin	France
SIDE – Michelin Développement France	France
Société d'Investissements et de Mécanique	France
Société Financière des Procédés Industriels	France
Société Nationale des Etablissements Piot Pneu	France
Spika	France
Transityre France	France
ViaMichelin	France
Elastika Michelin A.E.	Grèce
Michelin Central Europe Commercial Private Company Limited by Shares	Hongrie
MICHELIN Economy Developing Non-Profit Limited Liability Company	Hongrie
Michelin Hungaria Tyre Manufacture Ltd.	Hongrie
Taurus Carbonpack Commercial and Supplying Ltd.	Hongrie
Mireis Limited	Irlande
Miripro Insurance Company Limited	Irlande
Oboken Limited	Irlande
Fondazione Michelin Sviluppo	Italie
Società per Azioni Michelin Italiana	Italie
ViaMichelin Italia S.r.1.	Italie
Michelin Riepas SIA	Lettonie
UAB Michelin Padangos	Lituanie
Michelin Invest Luxembourg SCS	Luxembourg
Michelin Luxembourg SCS	Luxembourg

Razón Social	País
Norsk Michelin Gummi AS	Norvège
Actor B.V.	Pays-Bas
Eurodrive Services and Distribution N.V.	Pays-Bas
Euromaster Bandenservice B.V.	Pays-Bas
Euromaster Netherlands B.V.	Pays-Bas
Laurent Banden B.V.	Pays-Bas
Michelin Research Asia B.V.	Pays-Bas
MC Projects B.V.	Pays-Bas
Michelin Distribution B.V.	Pays-Bas
Michelin Finance (Pays-Bas) B.V.	Pays-Bas
Michelin Nederland N.V.	Pays-Bas
Soparin B.V.	Pays-Bas
Transityre B.V.	Pays-Bas
Viborg B.V.	Pays-Bas
Euromaster Polska sp. z.o.o.	Pologne
EUROMASTER PORTUGAL - SOCIEDADE UNIPESSOAL, LDA	Portugal
Michelin Development Foundation (Fundacja Rozwoju Michelin)	Pologne
Michelin Polska S.A.	Pologne
Michelin-Companhia Luso-Pneu, Limitada	Portugal
Fundatia Michelin Dezvoltare	Roumanie
Michelin Romania S.A.	Roumanie
Associated Tyre Specialists (Investment) Limited	Royaume-Uni
Associated Tyre Specialists Limited	Royaume-Uni
ATS Euromaster Limited	Royaume-Uni
ATS Cymru Wales Limited	Royaume-Uni
ATS Midlands Limited	Royaume-Uni
ATS North Eastern Limited	Royaume-Uni
ATS North Western Limited	Royaume-Uni
ATS Scotland Limited	Royaume-Uni
ATS Southern Limited	Royaume-Uni
ATS Western Limited	Royaume-Uni
ATS (IOM) Limited	Royaume-Uni
Baldovie Training Limited	Royaume-Uni
Michelin APA Publications Limited	Royaume-Uni
Michelin Development Limited	Royaume-Uni
Michelin Europe (EEIG)	Royaume-Uni
Michelin Finance (U.K.) Limited	Royaume-Uni
MichelIn Lifestyle Limited	Royaume-Uni
Michelin Services Ltd	Royaume-Uni
Michelin Tyre Public Limited Company	Royaume-Uni
ViaMichelin UK Limited	Royaume-Uni
LLC "Michelin Russian Tyre Manufacturing Company"	Russie
TIGAR TYRES d.o.o. Pirot	Serbie
MCSyncro Bratislava, s.r.o.	Slovaquie (Rép)
Michelin Slovensko, s.r.o.	Slovaquie (Rép)
Michelin Slovenija, pnevmatike, d.o.o.	Slovénie
Däckhuset i Skellefteå AB	Suède

Razón Social	País
Euromaster AB	Suède
Fastighetspolarna AB	Suède
Hjulsystem MCP AB	Suède
I Thunberg Trading AB	Suède
Landbloms Gummiverkstad K G Bohman AB	Suède
Leanders Gummiverkstad AB	Suède
Michelin Nordic AB	Suède
Norks Däckservice AB	Suède
Svahns Däckservice SOG AB	Suède
Compagnie Financière Michelin	Suisse
Euromaster (Suisse) SA	Suisse
Michelin Finanz Gesellschaft für Beteiligungen AG / S.A. / Limited	Suisse
Michelin Inter Assistance S.A. / AG / Limited	Suisse
Michelin Invest S.A. / AG / Limited	Suisse
Michelin Recherche et Technique S.A. / AG / Limited	Suisse
Michelin Suisse S.A. / AG / Ltd.	Suisse
Michelin Trésorerie Europe S.A. / AG / Ltd.	Suisse
Michelin Trésorerie Europe de l'Est S.A. / AG / Ltd.	Suisse
Nitor S.A. / AG / Limited	Suisse
MC Syncro Kolín s.r.o.	Tchéquie (Rép.)
Michelin Ceská republika s.r.o.	Tchéquie (Rép)

Lista de Sociedades Importadoras

Razón Social	País
MCSyncro SOUTH AFRICA (PTY) LTD	Afrique du Sud
Michelin Tyre Company South Africa (Proprietary) Limited	Afrique du Sud
Michelin Algérie SPA	Algérie
Société d'Applications Techniques Industrielles	Algérie
Michelin Argentina Sociedad Anónima, Industrial, Comercial y Financiera	Argentine
Michelin Australia Pty Ltd	Australie
Michelin Espírito Santo - Comércio, Importações e Exportações Ltda.	Brésil
Plantações E. Michelin Ltda.	Brésil
Plantações Michelin da Bahia Ltda.	Brésil
Sociedade Michelin de Participações, Indústria e Comércio Ltda.	Brésil
Société Moderne du Pneumatique Camerounais	Cameroun
Michelin Development (Canada) Inc.	Canada
Michelin North America (Canada) Inc.	Canada
Michelin Retread Technologies (Canada) Inc.	Canada
Michelin Alberta ULC	Canada
Oliver Rubber Canada Limited	Canada
Michelin Chile Ltda.	Chili
Michelin Asia (Hong Kong) Limited	Chine
Michelin Asia-Pacific Export (HK) Limited	Chine
Michelin Asia-Pacific Import (HK) Limited	Chine
Michelin Asia-Pacific Import-Export (HK) Limited	Chine
Michelin (China) Investment Co., Ltd.	Chine
Michelin Shenyang Tire Co., Ltd.	Chine
Michelin Tire Research and Development Center (Shanghai) Co., Ltd.	Chine
Michelin (Beijing) Tyre Retreading Co., Ltd.	Chine
Shanghai Michelin Warrior Tire Co., Ltd.	Chine
Tyre Plus (Shanghai) Auto Accessories Trading Co., Ltd.	Chine
Industria Colombiana de Llantas S.A.	Colombie
Michelin Korea Co., Ltd.	Corée du Sud
Michelin del Ecuador S.A.	Equateur
CR Funding Corporation	Etats-Unis
Michelin Corporation	Etats-Unis
Michelin Mexico Properties, Inc.	Etats-Unis
Michelin North America, Inc.	Etats-Unis
Michelin Retread Technologies, Inc.	Etats-Unis
Oliver Rubber Company, LLC	Etats-Unis
Pelham 2 Corp.	Etats-Unis
Tire Centers, LLC	Etats-Unis

Razón Social	País
TW-Fitting-NA, LLC	Etats-Unis
ViaMichelin North America LLC	Etats-Unis
Riverside Leasing Limited	Iles Caïmans
Michelin India Private Limited	Inde
Michelin India Tyres Private Limited	Inde
Michelin India TamilNadu Tyres Private Limited	Inde
Michelin Research Asia Co., Ltd. (Michelin Research Asia Kabushiki Kaisha)	Japon
Nihon Michelin Tire Co., Ltd.	Japon
Michelin Malaysia Sdn. Bhd.	Malaisie
Michelin Services (S.E.A.) Sdn. Bdn.	Malaisie
Autopartes Internacionales de Queretaro, S.A. de C.V.	Mexique
Autopartes Internacionales de Guanajuato, S.A. de C.V.	Mexique
Coordinadora de Servicios Automotrices, S.A. de C.V.	Mexique
Industrias Michelin, S.A. de C.V.	Mexique
Michelin Mexico Holding, S.A. de C.V.	Mexique
Michelin Mexico Services, S.A. de C.V.	Mexique
Renovados Industriales de Querétaro, S.A. de C.V.	Mexique
Michelin Tyre Services Company Ltd.	Nigeria
M. Michelin & Company Limited	Nouvelle Zélande
Michelin Panama Corp.	Panama
Michelin del Perú S.A.	Pérou
Michelin Asia (Singapore) Co. Pte. Ltd.	Singapour
Michelin Asia-Pacific Pte Ltd	Singapour
Société des Matières Premières Tropicales Pte. Ltd.	Singapour
Michelin Chun Shin Ltd.	Taiwan
Michelin Research Asia (Thailand) Co., Ltd.	Thaïlande
Michelin Siam Company Limited	Thaïlande
Michelin Siam Group Co., Ltd.	Thaïlande
Michelin Thai Holding Co., Ltd.	Thaïlande
Siam Tyre Phra Pradaeng Co., Ltd.	Thaïlande
Michelin Lastikleri Ticaret A.S.	Turquie
Michelin Venezuela, S.A.	Venezuela
Michelin Vietnam Company Limited	Vietnam

ANEXO 2

OPERACIONES DE TRATAMIENTO AFECTADAS POR LAS BCR.

Las operaciones de tratamiento que se ven afectadas por las BCR se refieren al personal en general (sobre todo, los que trabajan en el departamento de personal y/o recursos humanos, que confeccionan la nómina, gestionan la formación y el desarrollo de la carrera profesional y la movilidad), proveedores, clientes, contactos (empleados, proveedores, periódicos, etc.), la Intranet del grupo, mensajería, organigrama, las redes de comunicación dentro del grupo, fichero de datos personales en relación con la actividad comercial de las empresas del grupo y la gestión del equipamiento de neumáticos para empleados, etc.

Las BCR regulan todas las transferencias de datos personales de la Unión Europea a los países situados fuera de la Unión Europea, exceptuando las situaciones en las que los datos sólo atraviesan el territorio de la Unión Europea.

Para el tratamiento con proveedores, clientes y contactos, los datos personales transferidos generalmente se refieren al nombre, apellidos, dirección de correo electrónico profesional, número de teléfono profesional, número de identificación y posición que ocupa.

Para los tratamientos que afectan al personal: nóminas, gestión administrativa y de formación, gestión de la carrera profesional y la movilidad de los empleados, mensajería, directorio, organigrama, Intranet, los datos transferidos se refieren a las categorías siguientes:

• A: identificación, (Nombres y apellidos, sexo, identificación, fecha y lugar de nacimiento),
• B: Núm. de la seguridad social, Número de Seguro Social para los expatriados y el número equivalente para el personal local.
• C: Estado civil.
• D: Servicio Militar
• E: Formación Distinciones-Diplomas.
• F: Dirección personal y profesional de correo electrónico.
• G: La categoría profesional.
• I: Medios de transporte.

Para la contratación, los datos transferidos se refieren a las categorías siguientes:

• A: Identificación.
• E: Formación Distinciones-Diplomas.
• F: Dirección personal y profesional de correo electrónico,
• G: Situación profesional.

Para el fichero de datos personales, los datos transferidos se refieren a las categorías siguientes:

• A: Identificación,
• F: Dirección personal y profesional de correo electrónico,
• I: Medios de transporte.

ANEXO 3

Comité de Privacidad

El Comité de Privacidad está compuesto por:

El Director de cada uno de los siguientes departamentos y/o su representante designado:

- Servicio grupo de Personal.
- Grupo de Servicio SI.
- Grupo de Seguridad Corporativa (MSG)
- Servicio Grupo legal.

El Comité de Privacidad estará presidida por el Director jurídico de Michelin.

El comité es responsable de la correcta aplicación de las BCR dentro del grupo, que supervisará y actualizará según sea necesario. El Comité define las directrices generales y las posibles revisiones de los cambios propuestos. También se encarga de tramitar las solicitudes sobre la aprobación de las BCR dirigidas a los "Privacy Officers" locales, así como las peticiones éstos a dicho Comité en relación con los incidentes y/o infracciones de la privacidad que puedan haber llegado a su conocimiento.

ANEXO 3.1

Descripción del Puesto

Privacy Officer

Cometido: Asegurar el control de riesgos relacionados con la protección de datos de carácter personal en aplicación de la LOPD.

Alcance: Todas las operaciones de tratamiento implementadas por el Responsable del tratamiento.

- Trabajar en conexión con los otros *Privacy Officer*.

- Establecer el guión de las operaciones y de las formalidades de proceso de acuerdo con la ley española.

- Dar consejos y recomendaciones, incluyendo a los responsables de los datos/ficheros, antes de que se pongan en ejecución las actividades correspondientes en las que se vean afectados datos de carácter personal.

- Coordinar las relaciones y la comunicación con los distintos departamentos/servicios responsables de las actividades.

- Elaboración de una lista de las operaciones de tratamiento de datos personales:

  + Elaborar la lista.
  + Su actualización conforme a la ejecución de las operaciones de tratamiento.
  + Modificación y publicación de la misma.

- Cada tres años verificar el cumplimiento de la ley del país y de las *Binding Corporate Rules* (Normas Corporativas Vinculantes del Grupo):

  + Prestar consejo y realizar recomendaciones, en particular en materia de seguridad, la información personal, derecho a la privacidad, confidencialidad de los datos, etc.
  + Mediar y alertar.
  + Crear y fomentar una cultura de protección de datos personales, contribuir a crear una política del grupo sobre esta materia.
  + Comprobar la aplicación de las *Binding Corporate Rules* y observancia de la ley.
  + Realizar valoraciones anuales.

- Organizar la red de trabajo de la zona país para la gente con la misma tarea.

ANEXO 4

NOTA SOBRE LOS PROCEDIMIENTOS INTERNOS DEL GRUPO MICHELIN.

Como parte de las garantías que Michelin implementa en sus BCR, asegura que la aplicación de los principios establecidos en las referidas BCR que se aplican a todas las entidades del grupo, son revisadas de forma regular y periódica.

Dentro de la organización creada por Michelin y en el marco de los procedimientos en vigor en el grupo Michelin, que no puede renunciar a ellas, las normas que deben aplicarse para lograr y perpetuar la aplicación de las BCR del grupo Michelin son los siguientes:

1. En general, la creación de una directiva grupo emitida por el Director del servicio grupo en cuestión se justifica cuando surge la necesidad de un cambio importante en el grupo debido a la existencia de un problema y/o riesgo que requiere de dirección a nivel de grupo.

El procedimiento de creación de una directiva grupo debe aplicarse e irá precedida cada directiva de una nota de presentación aprobada en todas las entidades del grupo (se adjunta el procedimiento de creación y nota de acompañamiento). En la práctica, los Gerentes de Servicio Grupo que emiten la Directiva debe distribuirla y velar por su ejecución y aplicación. Si hay un número limitado y es vital que se implemente, el Servicio Grupo emite las directivas de forma automática y es revisada anualmente por el Consejo Ejecutivo del Grupo. La vida útil de una directiva varía en función de los objetivos y el calendario para la creación de cada directiva. Por otra parte, el referencial en que la Directiva se basa es a largo plazo y aplicable a fin de alcanzar los resultados fijados por la misma.

2. En particular, las BCR Michelin que regulan la transferencia de datos personales de una entidad con sede en la Unión Europea hacia una entidad con sede en un Estado no miembro de la Unión Europea y/o que no proporciona un nivel aceptable de protección en términos de las necesidades de la comunidad, justifica la creación de una directiva grupo emitida por el Director del Departamento Legal del Grupo en relación con el desafío y/o los riesgos en juego. El Servicio Grupo Jurídico es por lo tanto responsable de la elaboración de la Directiva y referenciales en que se basa, garantizando así mismo el despliegue y su aplicación efectiva.

3. Los “Privacy Officers” nombrados en el Departamento Jurídico de cada país, son responsables de que la organización Michelin garantice la protección de datos personales dentro del grupo.

4. El Servicio Jurídico Grupo, que emite la directiva de grupo, es responsable de comprobar las normas que expida. Por lo tanto, los “Privacy Officers” comprueban que el tratamiento se ajusta a las normas internas del grupo Michelin sobre la base del Programa de verificación del cumplimiento que se adjunta más adelante.

En la práctica, los Responsables del tratamiento, es decir, los gerentes de departamentos afectados por las operaciones de tratamiento implementados en la empresa que garantizan el cumplimiento de las normas de la empresa, realizar inspecciones de 1 º nivel a intervalos regulares sobre la base de dicho programa.

Aproximadamente cada 3 años, los "Privacy Officers" se asegurarán la fiabilidad de las inspecciones de 1 º nivel realizado por los responsables operacionales sobre la base del mencionado programa. Se elaborará un informe que se enviará al Director General de protección de Datos, así como a las autoridades de inspección a petición de éstas.

Cada 5 años, el grupo Auditoría Michelin evaluará el cumplimiento de las inspecciones realizadas por los "Privacy Officers" con el fin de garantizar que los riesgos sean controlados.

ANEXO 4.1

Nota que acompañan a la Directiva:
Protección y transferencia de datos personales fuera de la Unión Europea

1 - Resumen de gestión.

¿Por qué BCR y Directiva del grupo?

Las BCR establecen un marco para las transferencias de datos de carácter personal dentro del grupo y garantizan que, conforme a la legislación de la UE, las personas que gozan de la protección de sus datos personales en Europa continúen beneficiándose de ella cuando sus datos salgan del territorio europeo para ser tratados fuera de la Unión Europea, en países que no proporcionan una protección adecuada. La Directiva del grupo permite aplicar a todas las entidades del grupo las normas que contiene.

¿Por qué ahora?

Las situaciones en las que se producen las transferencias internacionales de datos están aumentando, como por ejemplo: la centralización en una base de datos dentro del grupo.
Dado que las transferencias pueden ser numerosas y variadas, con las BCR se evita la celebración de un contrato por cada transferencia de datos. Estas reglas internas aseguran que el tratamiento se realiza garantizando de forma adecuada la protección de la privacidad y derechos humanos dentro de las empresas del grupo establecidas en países fuera de la Unión Europea que no proporcionan una protección adecuada.

2 - Resumen del estudio de viabilidad.

Acuerdos para la aplicación de la Directiva.

Para facilitar la aplicación de la legislación nacional y las BCR para la transferencia de datos personales fuera de la Unión Europea, se creará una organización con la creación de figura del "Privacy Officers", que es designado dentro de los servicios jurídicos de Michelin.

Los "Privacy Officers" será responsables de asegurar:

1. El cumplimiento de la ley en su país.
2. La aplicación de las BCR en cada país situado fuera de la UE. Obviamente, se presume que las disposiciones sobre protección de datos se aplican en países que ofrecen una protección adecuada.

¿Esto cubre un riesgo significativo?

Una transferencia de datos de una entidad europea que no cumple los requisitos establecidos por las leyes de protección de datos sería ilegal y podría, en este sentido, incurrir en responsabilidad el responsable del tratamiento.

¿Qué medios hay disponibles?

Los recursos disponibles están basados en función de la organización y en el cometido de los "Privacy Officers", que serán responsables de difundir una cultura de protección de datos así como también promover la conexión de cada departamento de cada entidad. El "Privacy Officer" tiene claramente definidas sus funciones que debe cumplir, además de establecer objetivos anuales.

3 – Aplicación.

3.1 Principios.

Estos principios están establecidos en la Directiva del grupo. Las entidades europeas del grupo y las no europeas que presenten un nivel adecuado de protección tienen obligaciones que deben cumplir cuando tratan datos personales que son o han sido transferidos.

3.2 enfoque.

Una aproximación que será parte del proceso de ejecución y rendición de cuentas

4 - Seguimiento y puesta a punto de la aplicación.

Los "Privacy Officers" llevarán a cabo dos revisiones al año para asegurar la aplicación y/o identificar las dificultades encontradas. Estos análisis serán enviados al Comité del Protección de Datos Personales.

ANEXO 4.1 Bis

Group Procedure: Control Group Directives

PURPOSE

This Group Procedure defines all the operations to prepare, implement and follow up on a Group Directive.

A Group Directive (DIR) contains the rules to be applied to obtain and perpetuate an important change, justifying management at the Group level. Its application is mandatory in all addressed entities. It commits the responsibility of the Group Service Director who issues it. Limited in number and of a mandatory implementation character, the application of Directives is the subject of systematic follow-up by the Group Service issuers and of annual review by the CEG.

SCOPE

This procedure is applicable not later than **30 June 2005** for any Directive prepared by a Group Service and implemented in an entity of the Group.

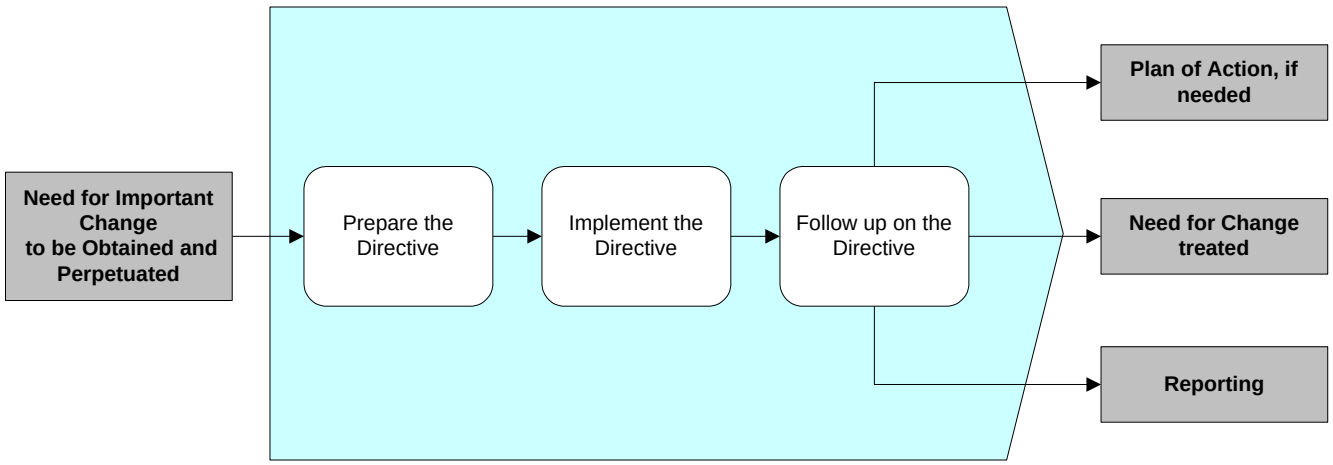
REFERENCE DOCUMENTS

DOCUMENTATION CONTROL 328 SGQ — PRG

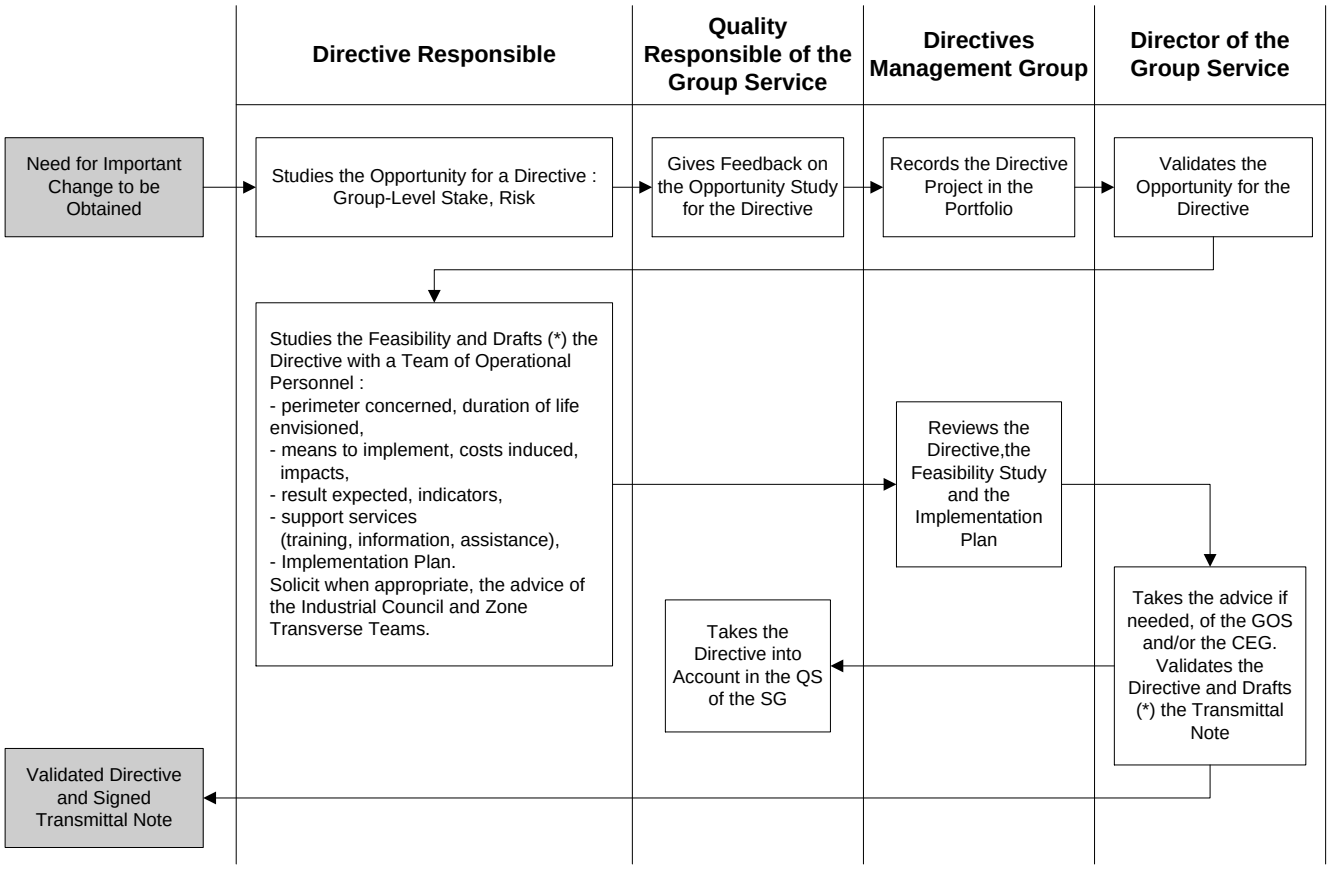
TEMPLATE FOR DRAFTING A DIRECTIVE

TEMPLATE FOR DRAFTING A TRANSMITTAL NOTE

LINKAGE OF ACTIVITIES

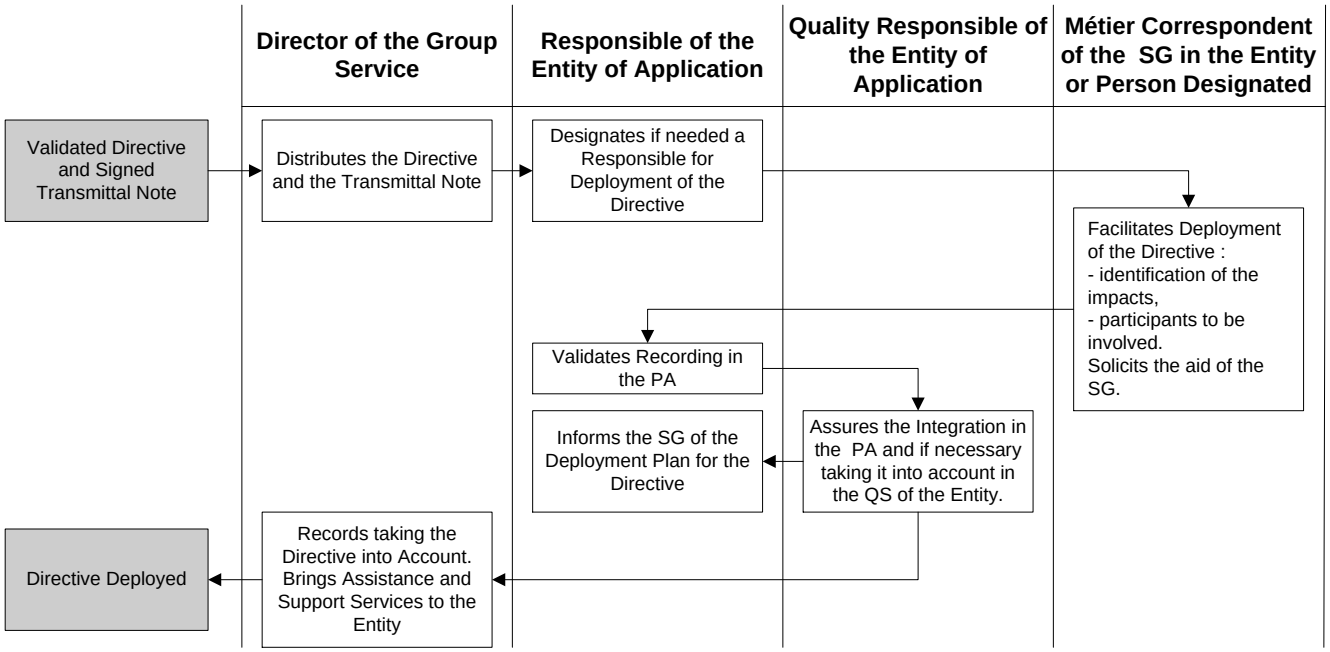


PREPARATION OF A DIRECTIVE

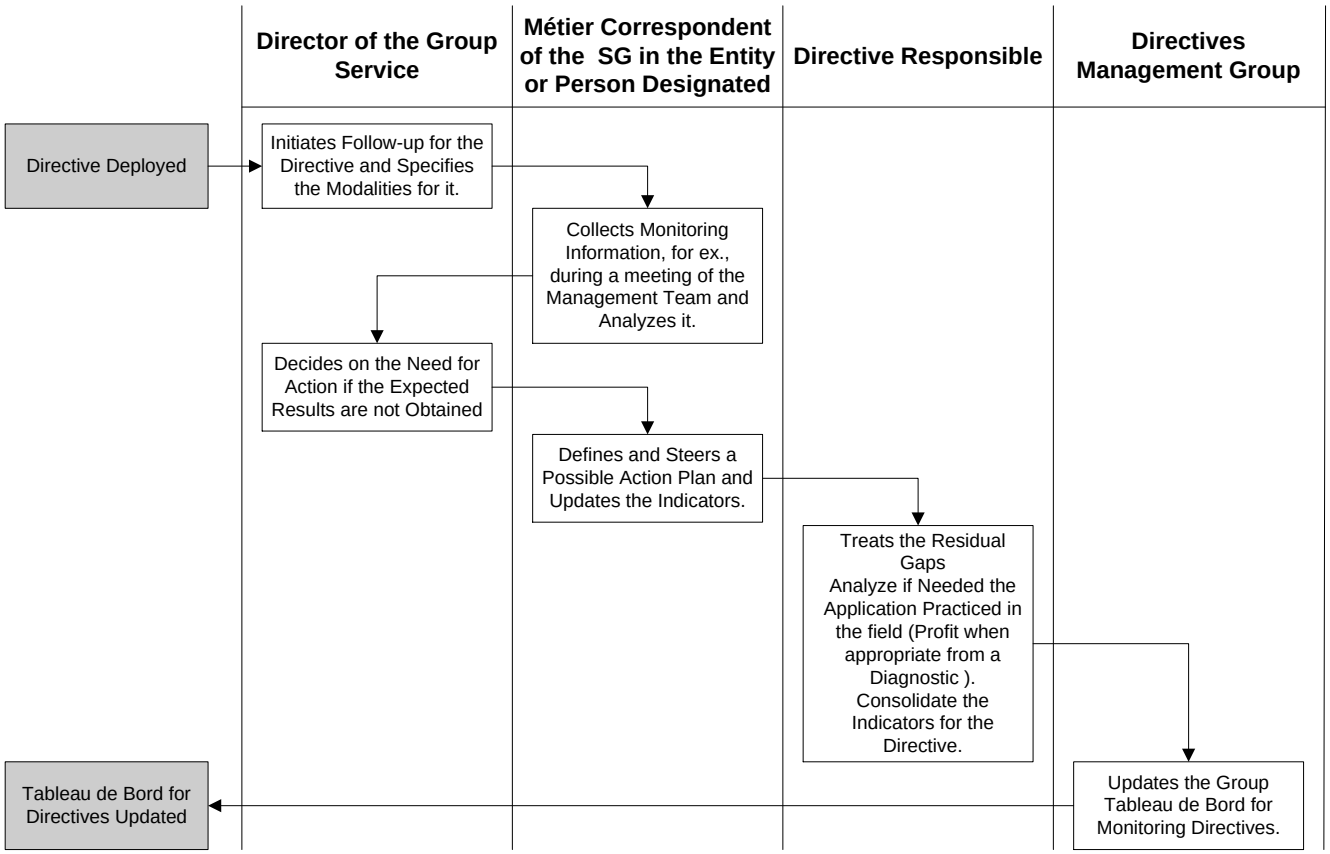


(*) : See document in reference

IMPLEMENTATION OF A DIRECTIVE



FOLLOW UP ON A DIRECTIVE



ANEXO 4.2

GROUP DIRECTIVE:
PROTECTION AND TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN UNION.

PURPOSE

The aim of this Group Directive is to implement and ensure the application of the following in all the countries where the Group operates:

- **national regulations for the protection of personal data and**
- **application by all the Group's entities of the binding corporate rules for the transfer of personal data from member states of the European Union to countries that do not provide an adequate level of protection.**

It stipulates the practical arrangements needed to meet requirements.

SCOPE

This Directive applies to all Group entities. It comes into force on 1 January 2009. Its purpose is to step up the effective roll-out of the binding corporate rules over the next two years, i.e. until 1 January 2011.

DEFINITIONS

.

The terms and expressions used in this Group Directive have the following meaning:

Personal data:

Any information relating to an identified or identifiable natural person (the data subject); a person is considered identifiable if he/she may be identified directly or indirectly particularly by reference to an identification number or one or more factors specific to his/her physical, physiological, psychological, economic, cultural or social identity.

Countries that provide an adequate level of protection:

1) member states of the European Union as well as 2) Liechtenstein, Norway and Iceland, 3) countries for which the European Commission has made an adequacy decision: Canada, Argentina, Switzerland, Isle of Man, Guernsey and/or 4) all countries that join the European Union and/or for which an adequacy decision will be made.

Processing of personal data:

Any operation or set of operations, whether performed or not using automated procedures, applied to personal data such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other type of publication, alignment or combination, blocking, erasure or destruction.

Transfer:

Any disclosure of personal data via a network or any disclosure from one medium to another, irrespective of the type of medium, in so far as such data is intended for processing in the recipient country.

PRINCIPLES

The founding principles of this directive are based on the Michelin Performance and Responsibility Charter, the security charter and Michelin binding corporate rules. They are intended to ensure an adequate level of protection as per European Directive 95/46 of 24 October 1995 when personal data is transferred from the Group's companies in the European Union to the Group's companies in countries that do not provide an adequate level of protection. The Group's companies to which data transfer relates must comply with the principles described in the binding corporate rules, i.e.

- Collect and process personal data fairly,
- Collect and transfer personal data for determined, explicit and legitimate purposes,

- Collect only accurate, adequate, relevant and non-excessive data for the purposes of the transfer,
- Only keep the data for the time needed to process the transfer,
- Set up adequate means of security and confidentiality to protect the data,
- Take the necessary steps to inform the people in question of the transfer of their data, processing of the data being transferred and the rights to which they are entitled,
- Take suitable steps, particularly by including appropriate clauses in the contracts in question to ensure that any subcontractors have implemented the necessary means of security and confidentiality to protect the data.

Arrangements for implementation and measurement of results

1. General organisation

A Data Protection Committee has been set up. It comprises SGD, SGSI, SGP and MSG managers. The committee will meet at least once a year. It is the body governing the protection of personal data. It will ensure that all the Group applies national legislation and binding corporate rules governing the transfer of personal data from the EU to countries that do not provide an adequate level of protection.

Privacy Officers are present in each legal department of the Michelin Group Companies. A network of Privacy Officers has been set up and is run by the Privacy Officers in France, North America, South America, Asia, Africa and the Middle East. These officers should inform the Data Protection Committee of any difficulties encountered and/or the issues they would like the Committee to address.

Interfaces are appointed in each department that implements personal data processing. They act as the interface with the Privacy Officers and people responsible in their entity for the processing to be implemented.

2. Awareness raising

A group memo will be distributed in December 2008 on the protection of personal data and the organisation in place. The awareness-raising programme will be adopted nationally and distributed via the various countries' intranets. In European countries, a guide comprising practical sheets will be uploaded onto the various countries' intranets with questions/answers. The countries are responsible for organising awareness-raising campaigns and may take any appropriate steps to increase employee awareness in their entity.

3. Training

Privacy Officers are responsible for training the managers of entities that implement processing of personal data and teams that process and/or use the data. The Privacy Officers must also ensure the traceability of the training given.

4. Application of quality assurance

Privacy Officers will apply quality assurance to the protection of personal data in their own country. To achieve this, they must draw up:

- Guidelines and recommendations,
- A code of conduct including sections such as:
  - Emergency and alert procedures,
  - Complaint management,
  - Any other sections they consider necessary.

5. Promoting the Personal Data Protection culture

- Particularly via memos.

6. Measurement of results

An annual assessment of the campaigns implemented by each Privacy Officer will be drawn up and sent to the Personal Data Protection Committee. The Interfaces and Privacy Officers will meet once a year to define any training schemes that may be necessary, guidelines to be drawn up, procedures to be implemented, etc. Results will be measured in compliance with legal requirements and binding corporate rules by means of compliancy audits of operational managers' 1st level inspections. Privacy Officers will perform these audits approximately every 3 years.

ANEXO 5

PROGRAMA DE VERIFICACIÓN DEL CUMPLIMIENTO DE LAS BCR

	Formalidades Previas	Realizado		Observaciones	Plan de Acción
		Sí	No		
	Declaraciones enviadas a la autoridad de protección de datos				
	Copia del acuse de recibo				
	Solicitud de autorización				
	Autorización de las decisiones de la autoridad de control				
	Negativa de la autoridad de control				
	¿Tiene el país donde los datos son transferidos u nivel aceptable de protección?				
	¿El país donde los datos son transferidos reconoce un nivel de protección adecuado?				
	¿El país donde los datos son transferidos está localizado fuera de la UE?				

	Tipo y proporcionalidad de los datos	Realizado		Observaciones	Plan de acción
		Sí	No		
	¿Los datos recogidos lícitamente? i.e. ¿sin su conocimiento?				
	¿Son recogidos de forma legal? i.e. ¿Con su autorización?				
	¿Están determinados los fines del tratamiento de los datos?				
	¿Los fines son claros?				
	¿Los datos personales son adecuados y apropiados en relación con el propósito del tratamiento en virtud del cual se han recabado y tratados?				
	¿Los datos personales son excesivos en relación con el propósito del tratamiento en virtud del cual se han recabado y tratados?				
	¿Los datos personales son correctos?				
	¿Los datos personales están y son actualizados?				
	¿Para los datos que resultan inexactos o incompletos en cuanto a la finalidad para la cual fueron recopilados y tratados, el Responsable ha tomado medidas para asegurarse de que se ha				

	Tipo y proporcionalidad de los datos	Realizado		Observaciones	Plan de acción
		Sí	No		
	corregido?				
	¿Los datos personales están almacenados de tal manera que permite identificar a la persona en cuestión a lo largo del tiempo de almacenamiento estrictamente previsto en el tratamiento?				
	¿Están los datos almacenados por tiempo definido?				
	¿El periodo de almacenamiento está en consonancia con la finalidad del tratamiento?				
	¿Se han establecido medidas para asegurar el almacenamiento?				
	¿Existen tratamientos en vigor en la empresa de los que se deriven administración del almacenamiento de datos?				
	¿Los datos son borrados o destruidos una vez finalizado el tiempo previsto de almacenamiento?				

	Derechos de los Interesados	Realizado		Observaciones	Plan de acción
		Sí	No		
	¿Conocen los Interesados las condiciones para ejercer su derecho al acceso, rectificación, cancelación y oposición de sus datos?				
	¿Hay solicitudes de acceso, rectificación y cancelación de datos atendidas?				
	¿Hay solicitudes relacionadas con el derecho de oposición al tratamiento de datos por razones legítimas atendidas?				
	¿Hay solicitudes relacionadas con el derecho de oposición al tratamiento de datos con fines de prospección comercial atendidas?				

	Tratamiento de datos sensibles	Realizado		Observaciones	Plan de acción
		Sí	No		
	¿Incluyen datos sensibles en algún tratamiento?				
	¿El Interesado ha autorizado a que sus datos personales sean tratados?				
	¿El tratamiento en cuestión se justifica por una necesidad vital en la que está en juego una vida humana?				
	¿El Interesado ha hecho públicos sus datos de carácter personal sensibles?				
	¿El tratamiento es necesario para denunciar o ejercer un derecho de defensa ante un				

	Tratamiento de datos sensibles	Realizado		Observaciones	Plan de acción
		Sí	No		
	Tribunal?				
	¿El tratamiento es necesario para fines de medicina preventiva, diagnosis, salud, etc.?				

	Transparencia - Información relativa al Interesado vía transferencia	Realizado		Observaciones	Plan de acción
		Sí	No		
	Tipo de datos transferido				
	Identificación del primer Responsable				
	Propósito de la transferencia prevista				
	Identificación del Responsable de la transferencia concreta				
	¿Están definidas las categorías de destinatarios de datos con acceso a los mismos?				
	En relación con el propósito del tratamiento ¿son los destinatarios de datos apropiados para tener acceso a los datos personales?				
	¿Existe un derecho de acceso y rectificación de datos?				
	¿Están las oposiciones de				

	Transparencia - Información relativa al Interesado vía transferencia	Realizado		Observaciones	Plan de acción
		Sí	No		
	los Interesados evaluadas y tratadas apropiadamente?				

	Garantías	Realizado		Observaciones	Plan de acción
		Sí	No		
	¿Existen programas de formación?				
	¿Para el Personal?				
	¿Para el Encargado?				
	¿La información sobre la transferencia ha sido subida a la Intranet del grupo?				
	¿Ha sido emitida la información a través de una nota interna y / o cualquier otro medio?				

	¿Hay alguna transferencia posterior a algún país?	Realizado		Observaciones	Plan de acción
		Sí	No		
En su caso	¿Fueron los Interesados previamente informados?				
	¿Han sido informados de la entidad Exportadora de los datos?				
	¿Se ha especificado el país de destino?				
	¿Está especificada la categoría de los destinatarios de los datos?				
	¿Se ha firmado un contrato				

	¿Hay alguna transferencia posterior a algún país?	Realizado		Observaciones	Plan de acción
		Sí	No		
	entre el Exportador situado en la UE y la compañía externa localizada fuera de la UE, de acuerdo con las cláusulas contractuales típicas aprobadas por la Comisión Europea para la Responsable-Responsable?				
	¿Se ha firmado un contrato entre el Exportador situado en la UE y la compañía externa localizada fuera de la UE, de acuerdo con las cláusulas contractuales típicas aprobadas por la Comisión Europea para la Responsable-Encargado?				
	¿Se ha firmado un contrato entre el Exportador situado en la UE y el Encargado situado en la UE?				
En su caso	¿El Encargado dispone de garantías en términos de seguridad de los datos?				
	¿El Encargado dispone de garantías en términos de conformidad de los datos?				
	¿El contrato establece que el Encargado solo trata los datos de acuerdo con las instrucciones del Responsable?				
	¿EL Responsable verifica el cumplimiento de las medidas de seguridad del Encargado tal y como se establezca en el contrato?				

	Confidencialidad y seguridad de los datos	Realizado		Observaciones	Plan de acción
		Sí	No		
	¿El Responsable ha tomado medidas para asegurar la confidencialidad e integridad de los datos?				
	¿Los servidores en los que están almacenados los datos han protegido el acceso?				
	¿Hay un sistema de bloqueo de datos?				
	¿Existen medidas de protección contra el fuego?				
	¿El acceso a los PC está protegido con contraseñas?				
	¿Existen medidas de protección contra la intrusión externa a través de redes IT?				
	¿Hay procedimientos para encriptar las transferencias de datos?				
	¿Hay un procedimiento seguro de destrucción de datos?				
	¿Hay previsto un plan de emergencia?				
	En general ¿el grupo dispone de una política sobre seguridad y confidencialidad de los datos?				

	Quejas	Realizado		Observaciones	Plan de acción
		Sí	No		

	¿Han sido presentadas quejas relativas al derecho a la privacidad y los derechos fundamentales?				
	¿Existe un listado de expedientes sobre quejas?				
	¿Ha habido mediación?				
	¿Se ha encontrado una solución?				

	Modificaciones de las BCR	**Realizado**		**Observaciones**	**Plan de acción**
		Sí	**No**		
	¿Ha habido una suscripción para modificar las BCRs?				
	¿Ha sido notificada la autoridad de control de la modificación de las BCR?				
	¿Se ha actualizado la lista de entidades Importadoras situadas fuera de la UE?				

ANEXO 6

PROTECTION DES DONNEES PERSONNELLES

GUIDE A L'USAGE DU PERSONNEL

Edito par P. Legrez

L'évolution constante des technologies de l'information et de la communication et le souci permanent de Michelin de respecter la vie privée et les libertés des personnes exige que chacun de nous s'approprie les principes du droit fondamental de la protection des données.

La loi « Informatique et Libertés » modifiée par la loi du 6 août 2004 définit les principes à respecter lors de la collecte, du traitement et de la conservation des données à caractère personnel. Cette loi renforce les droits des personnes sur leurs données, prévoit une simplification des formalités administratives déclaratives et renforce tout en les précisant les pouvoirs de contrôle et de sanctions de la Cnil.

Ce guide pratique a été rédigé pour vous sensibiliser, vous informer et aider ceux qui chez MFPM créent et/ou utilisent des données à caractère personnel en mettant l'accent sur les principes clés à respecter pour leur création, les droits et obligations de chacun et les formalités à effectuer.

Vous pouvez télécharger ce document sur le site www.tamtam.fr

Philippe LEGREZ
Directeur Juridique du Groupe Michelin
Global Chief Privacy Officer

SOMMAIRE

FICHE 1 : Qu'est-ce qu'un traitement régi par la loi Informatique et Libertés

Les traitements automatisés ou les fichiers manuels de données à caractère personnel dont le responsable est établi sur le territoire français ou recourt à des moyens de traitement situés sur ce territoire sont régis par la loi Informatique et Libertés du 6 janvier 1978, modifiée par le loi du 6 août 2004.

◆ Qu'est-ce qu'un traitement ?

Toute opération portant sur des données « quel que soit le procédé technique utilisé », telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la transmission, l'interconnexion de données à caractère personnel,…

Attention : Ne sont pas concernés par la loi, les traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles telles que les agendas électroniques, les répertoires personnels, …)

◆ Qu'est-ce qu'un fichier ?

Tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

◆ Qu'est ce qu'une donnée à caractère personnel ?

Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Attention : Des données que vous pourriez considérer comme anonymes peuvent constituer des données à caractère personnel si elles permettent d'identifier indirectement ou par recoupement d'informations une personne précise (exemples : date et lieu de naissance, adresse et profession des parents).

◆ Qui est le responsable de traitement ?

Le responsable de traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

Le responsable doit être établi sur le territoire français ou recourir à des moyens de traitement situés sur ce territoire.

Exemple : Le responsable du service du personnel France est responsable des traitements dont il a décidé la création, qui a déterminé à quoi il va servir et selon quelles modalités.

FICHE 2 : Quelles conditions doit respecter un traitement ?

A la création du traitement

Les 5 règles d'or à respecter

- respecter le principe de **finalité et de proportionnalité** : le traitement doit avoir une finalité déterminée, explicite et légitime et les données, collectées de manière loyale et licite, doivent être pertinentes au regard de cette finalité ;

- conserver les données pendant une **durée limitée** fixée en fonction de la finalité du traitement ;

- assurer la sécurité et la confidentialité des données ;

> *Exemple* : Les données ne doivent pas être déformées, endommagées ou être accessibles à des tiers non autorisés.

- **informer la personne** du traitement dont elle fait l'objet et de ses caractéristiques afin de lui permettre d'exercer ses droits d'accès, de modification, de suppression et d'opposition ;

> *Attention :* Le responsable de traitement doit obligatoirement informer les personnes concernées de leurs droits et identifier clairement le service auprès duquel s'exercent ses droits dans l'entreprise.

- **Déclarer le traitement auprès de la Cnil** et obtenir un numéro d'enregistrement avant sa mise en œuvre, sauf si un Cil (Correspondant Informatique et Libertés) a été désigné.

> *Attention :* Le responsable du traitement s'engage à réaliser une déclaration conforme à la réalité du traitement mis en œuvre.

Conditions propres aux données sensibles

Les données sensibles sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

Par principe, il est interdit de collecter et de traiter ce type de données.

Toutefois, la loi prévoit certaines dérogations. Ainsi la Cnil peut,autoriser, compte tenu de leur finalité, certains traitements si les données sont à bref délai, anonymisées selon un procédé reconnu conforme, au cas par cas, par la Cnil ou si les traitements sont justifiés par un intérêt public.

Pendant l'exploitation du traitement

Les données doivent être mises à jour ;

- La réutilisation des données pour une autre finalité est interdite sauf pour les traitements à des fins statistiques, historiques ou de recherche scientifique et sous réserve de :

  - ne pas être utilisées pour prendre des décisions à l'égard des personnes concernées ;

- et de respecter les conditions de la loi (finalité et proportionnalité, durée limitée, sécurité, information des personnes…).

Les transferts de données

- Vers un état appartenant à la Communauté européenne :

  Les transferts ne soulèvent pas de difficulté particulière, s'ils ont été prévus dans la déclaration initiale. A défaut, une modification de la déclaration est nécessaire.

- Vers un état n'appartenant pas à la Communauté européenne :

  Les transferts de données à caractère personnel ne sont possibles que si les états destinataires assurent un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes concernées par le traitement. A défaut, il convient de solliciter l'autorisation de la Cnil ou de respecter les conditions prévues par la loi.

En pratique : Si vous envisagez un tel transfert, contactez le Privacy Officer/CIL désigné pour la France et pour plus de détails, reportez vous à la fiche 6.

A l'expiration de la durée de conservation des données prévue pour le traitement

Il est interdit de réutiliser les données collectées et traitées à l'expiration de la durée de conservation prévue pour le traitement.

Au-delà de cette durée, les données doivent donc être détruites, effacées, supprimées ou archivées dans les conditions prévues par la réglementation applicable en matière d'archivage.

Les dérogations

Les données collectées peuvent être conservées au-delà de la durée nécessaire aux finalités initiales en vue d'être traitées à des fins historiques, statistiques ou scientifiques, sous réserve de respecter les conditions de la loi (finalité et proportionnalité, durée limitée, sécurité, information des personnes…).

FICHE 3 : Quels droits pour les personnes concernées ?

Toute personne auprès de laquelle sont recueillies des données à caractère personnel ou qui est concernée par un traitement dispose d'un droit à l'information, d'un droit d'accès, d'un droit d'opposition, d'un droit de rectification.

Qu'est-ce que le droit à l'information ?

C'est le droit pour toute personne de savoir si des données la concernant font l'objet d'un traitement et d'obtenir du responsable du traitement des informations sur celui-ci.

- **Les informations à transmettre systématiquement à la personne concernée sont :**

  - l'identité du responsable du traitement;
  - la finalité poursuivie par le traitement ;
  - le caractère obligatoire ou facultatif des réponses ;
  - les conséquences éventuelles, à son égard, d'un défaut de réponse ;
  - les destinataires de données ;
  - les droits d'accès, d'opposition et de rectification ;
  - les transferts de données envisagés à destination d'un état non membre de la Communauté Européenne.

En pratique : Les informations peuvent être délivrées par tous moyens, par exemple :
- par courrier électronique ou lettre d'information ;
- par affichage dans les locaux recevant les personnes concernées ;
- par mention sur un questionnaire, un formulaire de collecte de données en ligne ;
- au cours d'un entretien individuel….
- sur le site Tam-Tam France

En pratique : Des modèles de note d'information sont disponibles sur le site de tam tam.fr :

- **Lorsque les données sont recueillies directement auprès de la personne, ces informations doivent lui être délivrées par le responsable du traitement.**

- **Si les données sont recueillies par voie de questionnaire, les informations suivantes doivent en outre être mentionnées sur le questionnaire :**

  - l'identité du responsable du traitement;
  - la finalité poursuivie par le traitement ;
  - le caractère obligatoire ou facultatif des réponses ;
  - les conséquences éventuelles à son égard d'un défaut de réponse ;
  - les droits d'accès, d'opposition et de rectification.
  - les transferts de données envisagés à destination d'un pays non membre de l'Union Européenne.

- **Lorsque les données ne sont pas recueillies auprès de la personne concernée, toutes les informations relatives au traitement citées en préalable, doivent être fournies à la personne concernée dès l'enregistrement des données ou, si une communication de ces données à des tiers est envisagée, au plus tard lors de la première communication.**

Exemple : C'est le cas si les données sont recueillies directement auprès du responsable d'un autre traitement.

- **Lorsque les données ont été initialement recueillies pour un autre objet, toutes ces informations doivent également être fournies à la personne concernée, sauf si :**

  - la personne concernée est déjà informée ;
  - son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

Attention : L'impossibilité d'informer les personnes concernées doit pouvoir être justifiée auprès de la CNIL.

- **Lorsque les données sont appelées à faire l'objet dans un bref délai d'un procédé d'anonymisation, les informations qui doivent être délivrées à la personne concernée peuvent se limiter à l'identité du responsable du traitement et à la finalité poursuivie par le traitement.**

Qu'est-ce que le droit d'accès ?

Toute personne a le droit d'obtenir communication des données la concernant enregistrées dans le fichier sous une forme accessible et en obtenir une copie. (Article 39 de la loi)

Les informations qui doivent être communiquées.

Toute personne peut interroger le responsable d'un traitement de données à caractère personnel et obtenir sans justification :

- la confirmation que des données la concernant font l'objet ou non d'un traitement ;
- des informations relatives à la finalité du traitement, aux catégories de données et aux destinataires de ces données ;
- la communication des données qui la concernent ainsi que toute information sur l'origine de celles-ci;
- des informations sur les transferts de données envisagés à destination d'un Etat non membre de l'Union Européenne.

Recommandation : La réponse doit être faite par écrit.

Les modalités d'exercice du droit d'accès.

Le droit d'accès s'exerce auprès du service, responsable du traitement.

Il est tenu d'y faire droit sauf si la demande est manifestement abusive (par son caractère répétitif ou systématique).

Attention : Seul le coût de la reproduction de la copie des données peut être facturé.

Qu'est-ce que le droit d'opposition ?

Toute personne peut s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. (Article 38 de la loi)

Lorsque ces données sont destinées à être utilisées par le responsable du traitement à des fins de prospection, notamment commerciale, le droit d'opposition peut être exercé sans motif.

- **Qu'est-ce que le droit de rectification ?**

Toute personne peut exiger du responsable d'un traitement que soient rectifiées, complétées, mises à jour, verrouillées ou effacées les données la concernant qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation sont interdites. (Article 40 de la loi)

Attention : Lorsqu'une personne en fait la demande, le responsable du traitement doit justifier sans frais qu'il a procédé aux modifications demandées.

FICHE 4 : Quelles procédures vis-à-vis de la Cnil, pour quels traitements ?

- **Les procédures prévues par la loi**

C'est la finalité du traitement et la nature des données collectées qui déterminent le régime applicable au traitement (déclaration, autorisation ou avis préalables).

Le principe est celui de la déclaration préalable. Par conséquent, tous les traitements de données à caractère personnel doivent être déclarés préalablement à la Cnil avant leur mise en œuvre. Les traitements les plus courants peuvent être dispensés de déclaration ou faire l'objet d'une déclaration simplifiée s'ils respectent l'une des normes établies par la Cnil. Pour les entreprises qui ont désigné un Cil, les formalités de déclaration sont supprimées.

Attention : La désignation d'un Cil n'exonère pas les services et entités de Michelin de respecter les principes de la loi Informatique et Libertés dans la mise en oeuvre du traitement et de garantir les droits des personnes.

Pour les données sensibles, la biométrie, les transferts de données à caractère personnel vers des pays n'offrant pas un niveau de protection suffisant et les traitements susceptibles de porter atteinte aux droits et libertés des personnes limitativement énumérés par la loi, la mise en oeuvre de ces traitements est soumise à une **autorisation** de la CNIL ou à un acte réglementaire pris après avis de la CNIL.

Les traitements de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention sont soumis à des dispositions spécifiques de la loi. (Articles 62 à 66 de la loi.)

- **Les procédures internes à Michelin**

Tous les projets de traitement appelés à comprendre des données à caractère personnel, quelle que soit la procédure applicable, doivent être adressés au Privacy Officer qui a un rôle de :

- conseil, de veille et d'alerte en matière de déploiement de projets informatiques au sein de Michelin.
- de formation et de sensibilisation aux principes « *Informatique et Libertés* ».

En pratique : La liste des traitements par pays sera accessible sur le site tamtam.fr à la rubrique « données personnelles ».

FICHE 4.1 : Votre traitement comporte des données personnelles qui ne présentent pas de risques particuliers d'atteinte aux droits et libertés.

En principe :

Tous les traitements doivent faire l'objet d'une déclaration préalable auprès de la CNIL.

Dispense de déclaration

La Cnil peut dispenser de déclaration les traitements les plus courants :

Exemple : fichier paie
fichier fournisseurs comportant des personnes physiques
etc.

Déclaration simplifiée

Des normes ont été établies pour les traitements que la CNIL considère comme n'étant pas susceptibles de porter atteinte aux droits et libertés des personnes.

Si le traitement de données à caractère personnel est strictement conforme à l'une des normes établies par la CNIL, une déclaration simplifiée peut être mise en oeuvre.

Dans le cas contraire, le traitement de données à caractère personnel doit faire l'objet d'une déclaration normale auprès de la CNIL.

La déclaration normale

Une déclaration normale doit être faite si le traitement :

- n'est pas dispensé de déclaration ;
- n'est pas conforme aux normes simplifiées établies par la CNIL ;

- ne relève pas d'un autre régime (autorisation de la CNIL pour les données sensibles par exemple).

- **Le cas des sites internet**

Les sites internet doivent respecter la loi Informatique et Libertés s'ils comportent des données à caractère personnel.

Les sites internet ne font plus l'objet d'un formulaire spécifique de déclaration. Les traitements mis en oeuvre à partir d'un site internet peuvent relever selon leur finalité et la nature des données :

- d'une dispense de déclaration, pour les sites vitrines ou institutionnels collectant ou diffusant des données personnelles dans un but de communication ou d'information (abonnement à une lettre d'information, diffusion d'organigrammes, d'annuaires) et pour sites web personnels (blogs…) ;

- d'une déclaration simplifiée, pour les sites marchands ;

- et dans les autres cas, d'une déclaration normale, voir d'une demande d'avis ou d'autorisation.

- **Le cas des entreprises comme Michelin ayant désigné un Cil**

Les traitements rentrant dans ce cadre sont dispensés des formalités déclaratives ce qui ne veut pas dire que les obligations prévues dans la loi ne doivent pas être respectées. Le responsable du traitement n'est pas pour autant exonéré de ses responsabilités.

FICHE 4.2 : Votre traitement comporte des données présentant des risques particuliers d'atteinte aux droits et libertés

D'une manière générale, la finalité de ces traitements doit être clairement définie afin d'apprécier précisément la légitimité du recours à ce type de données à caractère personnel.

- **S'il s'agit de données sensibles**

Les données sensibles sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci.

Par principe, la collecte et le traitement de ces données sont interdits.

Cependant, dans la mesure où la finalité du traitement l'exige, ne sont pas soumis à cette interdiction :

- les traitements pour lesquels la personne concernée a donné son consentement exprès ;

- les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d'Etat.

La collecte et le traitement de ces données doivent dans ces hypothèses, être justifiés au cas par cas au regard des objectifs recherchés

- **Si le traitement comprend des données génétiques, des données pénales ou comporte des appréciations sur les difficultés sociales des personnes**

Dans tous ces cas, le traitement doit faire l'objet d'une autorisation de la CNIL.

- **Si le traitement comprend des données biométriques**

Une donnée biométrique est une donnée qui permet d'identifier un individu à partir de ses caractéristiques physiques, biologiques ou physiologiques.

Exemple : L'ADN, la rétine, l'iris, les empreintes digitales, le contour de la main, .la voix...

Les traitements de données à caractère personnel qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes sont soumis à autorisation de la CNIL.

- **Si le traitement comprend le numéro NIR ou nécessite la consultation du RNIPP**

Le numéro d'inscription des personnes (NIR) au répertoire national d'identification des personnes physiques (RNIPP), appelé encore numéro INSEE ou tout simplement numéro de sécurité sociale, est créé à partir de l'état civil et est géré par l'INSEE. Il permet l'identification de toute personne au moyen d'un numéro à 13 chiffres.

Recommandation de la CNIL :

La CNIL recommande que l'emploi du NIR comme identifiant des personnes dans les fichiers soit justifié et en aucun cas systématique et généralisé: (Délibération n° 83-058 du 29 novembre 1983 portant adoption d'une recommandation concernant la consultation du RNIP et l'utilisation du NIR)

- les responsables de la conception d'applications informatiques doivent donc se doter d'identifiants diversifiés et adaptés à leurs besoins propres ;

- la consultation du répertoire, qu'elle donne lieu ou non à utilisation du numéro d'inscription audit répertoire, doit être subordonnée à la conclusion de conventions spécifiques avec l'INSEE.

L'utilisation de ce numéro est toujours soumise à autorisation L'utilisation du NIR est soumise selon le cas, à une autorisation de la CNIL ou par décret en Conseil d'Etat pris après avis motivé et publié de la CNIL.

FICHE 5 : Recours aux sous-traitants

Comment les encadrer ?

Toute personne qui traite des données à caractère personnel pour le compte du responsable de traitement est un sous-traitant au sens de la loi du 6 janvier 1978 modifiée, dite loi Informatique et Libertés.

Par exemple : une société gérant un centre d'appels pour le compte du responsable de traitement est un sous-traitant.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité relatives aux données qui lui sont confiées. Il doit notamment empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès, obligation de sécurité qu'il partage donc avec le responsable du traitement.

Pour éviter toute ambiguïté, la loi précise même explicitement que cette obligation de sécurité du sous-traitant ne décharge pas le responsable du traitement de sa propre obligation de sécurité.

Pour formaliser cet aspect, le contrat liant le sous-traitant au responsable du traitement doit comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et doit prévoir que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

Il faut donc s'assurer que les sous-traitants présentent des garanties suffisantes en matière de sécurité.

Tout contrat informatique par lequel le client responsable d'un traitement de données à caractère personnel confie de manière directe ou indirecte à un prestataire le traitement de ces données doit comporter des dispositions en matière de sécurité physique et logique de données.

1. Lorsque le sous-traitant est établi en France et/ou dans l'Union Européenne, le contrat doit comporter une clause spécifique sur la caractère confidentiel des données et sur les précautions qui doivent être prises afin de préserver la sécurité des données et empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

2. Lorsque le sous-traitant est établi en dehors de l'Union Européenne, le responsable de traitement établi dans l'Union Européenne à l'origine du transfert de données, devra établir un contrat pour encadrer le transfert et reprendre les clauses contractuelles type adoptées par la Commission Européenne dans sa décision n° 2002/16/CE en date du 27 décembre 2001 (Transfert de responsable de traitement à sous-traitant).

FICHE 6 : Les transferts de données

Qu'est-ce qu'un transfert ?

Toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données, d'un support à un autre, dans la mesure ou ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire.

Le principe :

Interdiction du transfert vers les Etats n'accordant pas une protection adéquate de la vie privée et des libertés et droits des personnes.

- Nécessité d'une protection suffisante dans le pays d'établissement du destinataire :
  - pays de l'Union Européenne
  - pays de l'Espace Economique Européen
- reconnaissance du caractère suffisant :
  - Argentine, Canada, Ile de Man, Suisse, Guernesey, USA pour les entreprises ayant adhérer aux Safe Harbor).

Des exceptions au principe d'interdiction du transfert vers les Etats n'accordant pas une protection adéquate de la vie privée et des libertés et droits des personnes :

- le consentement
- si le traitement est nécessaire à la sauvegarde de la vie humaine
- la sauvegarde de l'intérêt public
- le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice
- la consultation dans des conditions régulières d'un registre public
- l'exécution d'un contrat entre le responsable de traitement et l'intéressé
- la conclusion ou l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable de traitement et un tiers.
- le transfert autorisé par la Cnil sur la base **:**
  - d'un contrat reprenant les clauses types de la Commission Européenne :

- de responsable, de traitement à responsable de traitement
- de responsable de traitement à sous-traitant

- de règles internes d'entreprise qui constituera la norme interne de référence applicable à toutes les entités du groupe.

  Michelin a opté pour cette solution et dispose de Règles Internes d'Entreprise (Binding Corporate Rules en anglais) accessibles sur le site intralegal.michelin.com.

  La procédure d'autorisation de la Cnil permettant à Michelin d' opérer des transferts de données à partir de la France vers des pays non membres de l'UE est en cours. Les transferts à l'intérieur de l'UE, EEE et vers les pays ayant fait l'objet d'une décision d'adéquation sont libres.

FICHE 7 : La CNIL et ses pouvoirs

La CNIL est une autorité administrative française chargée de veiller au respect de la loi Informatique et Libertés. Dans chaque état membre de l'Union Européenne, il y a une autorité administrative indépendante.

- **Elle a des devoirs et des pouvoirs :**

  - **Informer**

    La CNIL informe les personnes de leurs droits et obligations et propose au gouvernement les mesures pour adapter la protection des libertés et de la vie privée à l'évolution des techniques.

  - **Contrôler**

    La CNIL veille à ce que les traitements soient mis en oeuvre conformément aux dispositions de la loi. Elle use de ses pouvoirs de vérification et d'investigation pour instruire les plaintes et surveiller la sécurité des systèmes d'information.

  - **Sanctionner**

    La CNIL peut prononcer diverses sanctions (avertissement, mise en demeure, sanction pécuniaire, injonction de cesser le traitement, ...). Elle peut demander aux juridictions compétentes d'ordonner toute mesure de sécurité nécessaire et dénoncer les violations de la loi.

  - **La Cnil donne des avis**

    Elle autorise ou donne un avis sur les traitements de données sensibles à caractère personnel et reçoit les déclarations des autres traitements. La Cnil tient à la disposition du public la liste des traitements déclarés et leurs principales caractéristiques.

- **Elle réglemente**

Afin d'alléger les déclarations, la CNIL peut établir des normes simplifiées pour les traitements les plus courants et les moins dangereux pour les droits et libertés des personnes. Elle peut également décider de dispenser de toute déclaration préalable les traitements ne présentant pas de risque d'atteinte aux droits et libertés.

FICHE 8 : Les sanctions

- **Les sanctions pénales en cas de violation des règles relatives à :**

Sous-traitance	5 ans de prison 300 000 €
absence de formalités déclaratives;	
communication d'informations à des personnes non autorisées ;	
mise en œuvre d'un traitement comportant des données à caractère personnel malgré l'opposition de celle-ci ;	
données à caractère personnel	
absence de mesures pour préserver la sécurité et la confidentialité des données ;	
conservation excessive - détournement finalité ;	
non-respect obligations déclaratives ;	
collecte frauduleuse, déloyale ou illicite ;	
traitement de données interdites ;	
Entrave aux actions de la Cnil ;	1 an de prison 15 000 €

- **Mais aussi sanctions administratives**

- par la Cnil
- jusqu'à 300 000 € d'amende

+ risque de responsabilité civile

LEXIQUE

- **Accès (droit d')**

Droit pour toute personne physique justifiant de son identité d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées, aux destinataires, à la confirmation que les données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement. Toute personne peut demander la communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci.

- **Biométrie**

Les données biométriques permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques ou physiologiques (ex. l'ADN, la rétine, l'iris, les empreintes digitales, la voix, …)

- **Collecter**

Il s'agit de recueillir des données à caractère personnel. Cette collecte peut s'effectuer notamment à l'aide de questionnaires ou de formulaires en ligne. Si cette dernière est effectuée à l'insu des personnes, la collecte est alors considérée comme déloyale.

- **Collecte directe**

Données à caractère personnel recueillies directement auprès de la personne concernée.

- **Collecte indirecte**

Données qui n'ont pas été recueillies directement auprès de la personne concernée. Dans ce cas, le responsable du traitement ou son représentant doit fournir à cette dernière les informations dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

- **Conservation**

  Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. La Cnil détermine des durées de conservation de référence dans le cadre de ses dispenses de déclaration et normes simplifiées qui doivent être respectées pour pouvoir en bénéficier.

- **Privacy Officer (CIL)**

  Personne physique ou morale, désignée par Michelin chargée d'assurer le respect des obligations prévues par la loi Informatique et libertés. Une telle désignation entraîne la dispense des formalités de déclaration normale et simplifiée pour les traitements en relevant sauf si ces traitements prévoient un transfert de données à destination d'un Etat non membre de l'Union européenne pour lesquels une autorisation de la Cnil est requise.

- **Destinataire de données**

  Toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

- **Données à caractère personnel**

  Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

- **Données sensibles**

  Données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

- **Exportateur de données**

Le responsable du traitement qui transfère les données à caractère personnel

- **Fichier de données à caractère personnel**

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

- **Importateur de données**

Le responsable du traitement qui accepte de recevoir de l'exportateur des données à caractère personnel en vue de leur traitement ultérieur. L'importateur des données doit être soumis à un certain nombre d'obligations pour garantir notamment la sécurité des données, la finalité du traitement.

- **Information**

La personne auprès de laquelle sont recueillies les données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

- de l'identité du responsable du traitement;
- de la finalité poursuivie par le traitement auquel les données sont destinées ;
- du caractère obligatoire ou facultatif des réponses ;
- des conséquences éventuelles, à son égard, d'un défaut de réponse ;
- des destinataires ou catégories de destinataires des données ;
- des droits qu'elle tient des dispositions de la loi Informatique et libertés (section 2 du chapitre V) ;
- le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union Européenne.

Il est à noter que, si de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions énumérées à l'article 32 de la loi Informatique et libertés.

- **Interconnexion**

Une interconnexion de fichiers consiste à mettre en relation des fichiers relevant d'une ou plusieurs personnes et dont les finalités peuvent être identiques, différentes ou complémentaires. L'interconnexion consiste notamment à alimenter un fichier par un autre fichier, à une fusion de fichiers,

à mettre en relation plusieurs fichiers normalement gérés séparément ou à alimenter une base de données à partir de plusieurs fichiers.

- **Maître du fichier**

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées

- **NIR / N° INSEE / N° de sécurité sociale**

Le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (RNIPP) appelé encore numéro INSEE, ou tout simplement numéro de sécurité sociale est créé à partir de l'état civil et est géré par l'INSEE. Il permet l'identification de toute personne au moyen d'un numéro de 13 chiffres. L'utilisation de ce numéro est toujours soumise à autorisation. Le NIR est composé de 13 chiffres : le sexe (1 chiffre), l'année de naissance (2 chiffres), le mois de naissance (2 chiffres) et le lieu de naissance (5 chiffres ou caractères) de la personne concernée. Les 3 chiffres suivants correspondent à un numéro d'ordre qui permet de distinguer les personnes qui auraient 10 premiers chiffres identiques.

- **Opposition (droit d')**

Droit pour toute personne physique « de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Ce droit s'exerce sans frais lorsque les données la concernant sont utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur »

- **Personne concernée par un traitement**

Personne à laquelle se rapportent les données qui font l'objet du traitement

- **Proportionnalité**

Le traitement d'informations nominatives doit être proportionné à la finalité déclarée, c'est-à-dire qu'il doit s'effectuer de façon adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi. Les droits et libertés ne peuvent être restreints que si cette restriction est justifiée par la nature des tâches à accomplir et proportionnée aux buts recherchés.

- **Protection adéquat (niveau de protection)**

  Niveau de protection de données à caractère personnel faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement offert par un pays. Ce niveau est apprécié quand les informations doivent être transférées dans un pays tiers à l'Union européenne. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie en considération de la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

- **Protection suffisant (niveau de)**

  Niveau de protection de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement devant être assuré par un Etat n'appartenant pas à l'Union européenne afin que le responsable du traitement puisse transférer des données à caractère personnel vers cet Etat

- **Rectification**

  Droit pour toute personne physique justifiant de son identité d'exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation sont interdites. Si l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais, pour le demandeur, qu'il a procédé aux opérations exigées

- **Responsable de traitement de données à caractère personnel**

  Sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens d'un traitement.(ex : les responsables de service).

- **Sécurité des données**

  Assurer la sécurité des données, c'est pouvoir garantir la confidentialité des données qui y figurent et disposer en permanence d'un outil de travail fiable. La Cnil préconise l'adoption de mesures de sécurité physique et logique qui doivent être adaptées en fonction de l'utilisation qui est faite de l'ordinateur et sa configuration. Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès

- **Sous-traitant**

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instructions du responsable du traitement. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité. Cette exigence ne décharge pas pour autant le responsable du traitement de son obligation de veiller à la mise en oeuvre effective de ces mesures. Le contrat liant le sous-traitant au responsable du traitement doit comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et indiquer que le sous-traitant ne peut agir que sur instructions du responsable du traitement.

ANNEXES

- **Adresse/liens utiles**

www.cnil.fr

- **Documents de référence**

1. Textes fondamentaux

Textes internationaux et européens

- Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Textes législatifs

- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Textes réglementaires

- Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.
- Décret n° 2007-451 du 25 mars 2007 modifiant le décret du 20/10/2005.

2. Règles internes d'entreprise/ Binding Corporate Rules

http://intralegal.michelin.com/MondeFR/home/index.htm

3. Les clauses contractuelles type

Adoptées par la Commission Européenne dans sa décision n° 2002/16/CE en date du 27 décembre 2001 (Transfert de responsable de traitement à sous-traitant).

http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/CCT_ss_traitant_VF.pdf