THE DRINKS COMPANY
DISTRIBUCIONS TÚNEL S.A.

POLÍTICAS Y NORMAS DE PRIVACIDAD

Última actualización: Mayo 2018

Contenido

POLÍTICAS Y NORMAS DE PRIVACIDAD

Última actualización: Mayo 2018

1. Introducción

1.1. Objetivo

El presente documento recoge las políticas y normas de privacidad definidas por la organización con el objetivo de asegurar un adecuado cumplimiento de la normativa de protección de datos personales y especialmente de las obligaciones dispuestas por el Reglamento General de Protección de Datos – RGPD- (REGLAMENTO (UE) 2016/679).

Forma parte del modelo de gestión de cumplimiento del RGPD que la organización ha implementado para prevenir, detectar y mitigar riesgos para los derechos y las libertades de las personas físicas afectadas por los tratamientos de datos personales esta realiza.

Todos los niveles de la organización deben velar por el cumplimiento de dichas políticas y normas, así como de forma general con los procedimientos y medidas recogidos en el citado modelo de gestión y con la normativa vigente en materia de protección de datos.

1.2. Soporte organizativo y funciones

La organización cuenta con el oportuno soporte organizativo y ha definido las funciones necesarias para aplicar y controlar el cumplimiento de las políticas, normas y procedimientos definidos en materia de privacidad. Este soporte organizativo y estas funciones deben ser conocidas por los destinatarios del presente documento. A tal efecto la organización le comunicará o pondrá a su disposición esta información mediante los mecanismos o canales oportunos.

1.3. Destinatarios y aceptación

Las políticas y normas de privacidad recogidas en el presente documento o las que, en el futuro, se definan, vinculan a los administradores, directivos, trabajadores o personas en prácticas que desarrollen su actividad profesional en la organización, cualquiera que sea el vínculo jurídico que les una con la misma.

También vinculan a los colaboradores o usuarios externos con acceso a datos o sistemas de la organización.

El presente documento recoge normas de alcance general y normas específicas que afectan a determinados departamentos o perfiles.

Todos los niveles de la organización y los colaboradores o usuarios externos a la que se hiciese extensiva la aplicación del presente documento aceptan expresamente las normas y los principios de actuación que en él se establecen y se comprometen a consultar y cumplir cuantas instrucciones, decálogos o procedimientos de privacidad la organización les comunique o ponga a su disposición mediante los mecanismos o a través de los canales oportunos.

1.4. Régimen sancionador

El incumplimiento de las políticas y normas de privacidad será considerado como una infracción muy grave y dará lugar a la aplicación del procedimiento sancionador previsto por el convenio colectivo de aplicación. No obstante, si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del infractor o de la ilicitud del hecho, podrá rebajarse la gravedad de la infracción atendiendo a las circunstancias concretas del caso.

El incumplimiento de las políticas y normas de privacidad por parte de aquellas personas a las que se haya hecho extensiva la aplicación de las mismas, podrá ser motivo de resolución de la relación contractual que se haya formalizado con los interesados, sin perjuicio de cuantas acciones judiciales la organización estimase oportunas.

Las sanciones podrán graduarse atendiendo a la naturaleza y el contexto de la infracción, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados, y a cualquier otra circunstancia que sea relevante para determinar el grado de ilicitud y de culpabilidad presentes en la concreta actuación infractora.

2. Decálogos

(Véanse en las páginas siguientes)

POLÍTICAS Y NORMAS DE PRIVACIDAD

Última actualización: Mayo 2018

DECÁLOGO GENERAL

Todos los trabajadores, colaboradores o usuarios externos con acceso a datos personales o a sistemas de la organización deberán cumplir con las siguientes normas respecto al tratamiento de datos personales y seguridad de la información:

1. Debe conocer el soporte organizativo y las personas que asumen funciones para aplicar y controlar el cumplimiento de las políticas, normas y procedimientos definidos por la organización en materia de privacidad.

2. Para aquellos puestos en los que sea necesaria la recogida de información personal, esta se realizará siguiendo las pautas que se describen a continuación:

   - Únicamente se recabarán los datos necesarios para la finalidad perseguida.
   - Se hará lo posible para comprobar que los datos facilitados con correctos y veraces.
   - Se recogerán los datos utilizando los medios fijados por la entidad (impresos, formularios…), de forma que se garantice que el interesado recibe la información necesaria sobre el tratamiento de sus datos personales y que se recaben los consentimientos necesarios para los tratamientos a realizar y las posibles comunicaciones de datos que vayan a llevare a cabo.
   - Durante el proceso de recogida se guardará una actitud de discreción para evitar que la información recabada, especialmente en los casos en los que el interesado la facilite de manera verbal, sea conocida por terceros.

3. El uso que se haga de la información personal se regirá por las siguientes normas:

   - Los datos se tratarán únicamente para la finalidad para la que fueron recabados. Cualquier uso distinto al previsto inicialmente debe contar con el consentimiento del interesado.
   - En el tratamiento de la información se aplicarán las medidas de seguridad definidas por la organización.
   - En todo caso Ud. debe velar por la seguridad de la información en sus actuaciones cotidianas y evitar tratamiento o actitudes que puedan poner en peligro su confidencialidad, integridad o disponibilidad.
   - Cualquier incidencia que afecte a la seguridad de la información, a su confidencialidad o a su integridad, deberá notificarse a la persona que asume la función de Encargado del registro de incidencias o al responsable de su departamento.
   - Sobre toda la información tratada existe un deber general de secreto que afecta a todos los que intervienen en el tratamiento, sean empleados de la entidad o prestadores de servicios. Este deber de secreto permanece una vez finalizada la relación con la entidad.

4. No se comunicarán datos personales a terceros sin el consentimiento del interesado, salvo para el cumplimiento de obligaciones legales (Agencia Tributaria, Seguridad Social, jueces, etc.) o que el acceso a los datos sea necesario para la prestación de un servicio contratado por la organización.

5. Si su puesto requiere acceder o tratar datos de nivel alto, deberá cumplir con las normas indicadas en el decálogo para personas con acceso a datos de nivel alto. Son considerados como de nivel alto los siguientes datos:

- Datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical;
- Datos relativos a la salud, datos genéticos o datos biométricos;
- Datos relativos a la vida sexual o la orientación sexual;
- Datos relativos a condenas e infracciones penales.

6. No se dejará información abandonada, al alcance de terceros o personal ajeno a su departamento.
7. Únicamente podrá archivarse información en las áreas previstas para ello y mediante los criterios establecidos por la organización.
8. Únicamente podrán realizar tratamientos de datos fuera de la organización los usuarios autorizados expresamente para ello. Durante el transporte de documentos o soportes deberán adoptarse medidas para evitar el acceso no autorizado a los datos (sobres, maletines o cajas cerrados, o cualquier medida equivalente).
9. Para desechar cualquier papel o listado que contengan información personal, aunque solo sean nombres de pila, se hará uso de los medios de destrucción segura previstos por la organización, como por ejemplo destructoras de papel o contenedores de documentos confidencial.
10. Los bienes y recursos puestos a su disposición por la organización, especialmente los sistemas informáticos y de comunicaciones, no podrán usarse para fines distintos a los directamente relacionados con el desempeño de sus funciones en la organización.
11. Cuando se remitan e-mails con copia a otros destinatarios se utilizará siempre la opción de copia oculta (CCO……), salvo en el caso de correo interno o de ámbito estrictamente profesional.
12. En caso de recibir una solicitud de ejercicio de los derechos reconocidos por el RGPD por parte de un interesado, deberá ponerlo en conocimiento de la persona que asumen la función de Responsable para los Derechos RGPD o del responsable de su departamento.
13. Debe consultar y cumplir las instrucciones, decálogos y procedimientos que, en relación con su puesto de trabajo o funciones, la organización le haya proporcionado.
14. Ante cualquier duda, debe consultar al responsable de su departamento o al Responsable de Privacidad.

DECÁLOGO PARA PERSONAS CON ACCESO A DATOS DE NIVEL ALTO

Además del decálogo RGPD general, las personas que pueden acceder a datos de nivel alto deben cumplir las siguientes normas:

1. Son considerados como de nivel alto los siguientes datos:
   - Datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical;
   - Datos relativos a la salud, datos genéticos o datos biométricos;
   - Datos relativos a la vida sexual o la orientación sexual;
   - Datos relativos a condenas e infracciones penales.
2. Los usuarios sólo podrán acceder a documentos de nivel alto para el desempeño de sus funciones en el estricto cumplimiento de las tareas habituales asociadas a su puesto de trabajo, (p.ej. Creación y gestión de un expediente jurídico, gestión de incidencias, investigación de un accidente laboral, etc...). Cualquier acceso para la realización de tareas no habituales o por parte de terceros deberá ser autorizado y controlado por el responsable de su departamento. El acceso deberá asimismo ser registrado.
3. Sólo pueden realizarse copias y reproducciones de documentos de nivel alto para el desempeño de sus funciones en el estricto cumplimiento de las tareas habituales asociadas a su puesto de trabajo. Cualquier copia o reproducción que no se realice para el desarrollo de las citadas tareas habituales, será considerado como extraordinario y deberá ser autorizado, controlado y registrado por el responsable de su departamento. El acceso deberá asimismo ser registrado.
4. La entrada y salida de documentos de nivel alto deberá registrarse según el mecanismo de registro previsto a tal efecto en el departamento.
5. Salvo autorización específica, los datos de nivel alto no se podrán almacenar en sistemas informáticos locales.
6. Para la comunicación de documentos que contengan datos de nivel alto entre integrantes del departamento, se utilizarán carpetas compartidas del sistema. Únicamente se justificará el envío de datos de nivel alto por email, cuando el destinatario se encuentre fuera de las instalaciones. En todo caso, para los envíos por email, deberán aplicarse los mecanismos determinados por la organización para cifrar dichos datos, o la medida equivalente prevista a tal efecto.

DECÁLOGO PARA RESPONSABLES DE DEPARTAMENTOS

Además del decálogo RGPD general, los Responsable de departamentos de le organización cumplir las siguientes normas respecto al tratamiento de datos personales:

1. Con carácter previo y con la antelación necesaria, deberá imperativamente comunicar al Responsable de Privacidad cualquier proyecto que implique la realización de nuevos tratamientos de datos o cambios en tratamientos existentes en su departamento.

2. Quedan especialmente afectados, aunque de forma no limitativa, los siguientes tratamientos o cambios:

   - Tratamientos de datos a gran escala, por ejemplo:
     - Tratamientos de datos un número elevado de personas o, alternativa o adicionalmente, acumulación una gran cantidad de datos respecto de los interesados;
     - Utilización tecnologías de datos masivos (big data, Internet of things, etc.)
   - Tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical;
   - Tratamiento de datos genéticos, datos relativos a la salud;
   - Tratamiento datos biométricos dirigidos a identificar de manera unívoca a una persona;
   - Tratamiento datos relativos a la vida sexual o la orientación sexual de una persona física;
   - Tratamiento de datos relativos a condenas e infracciones penales;
   - Realización de perfiles, análisis o predicción de aspectos referidos al rendimiento en el trabajo, a la situación económica, a la salud, a preferencias o intereses personales, a fiabilidad o comportamiento, a solvencia financiera, localización o movimientos del interesado;
   - Monitorización y decisiones automatizadas,
   - Uso de tecnologías potencialmente invasiva, por ejemplo:
     - Videovigilancia a gran escala
     - Utilización de aeronaves no tripuladas (drones)
     - Vigilancia electrónica
     - Minería de datos
     - Biometría
     - Técnicas genéticas
     - Geolocalización
     - Utilización de etiquetas de radiofrecuencia o RFID
   - Observación de una zona de acceso público;
   - Transferencias de datos fuera del Espacio Económico Europeo;
   - Tratamiento de datos de personas vulnerables y, en particular, de menores de edad o personas con discapacidad;
   - Externalización de servicios.
   - Nuevas fuentes de datos o cambio en los procesos de recogida;
   - Cambios en las categorías de personas afectadas por el tratamiento o en los tipos de datos tratados;
   - Variación en las finalidades de los tratamientos;
   - Cambios en los flujos de datos;

- Cambios en los sistemas utilizados;
- Cambios en proveedores con acceso a datos personales;
- Cambios en los plazos de conservación de los datos por motivos operativos o legales.

3. Aplicará las medidas técnicas y organizativas apropiadas para que las actividades desarrolladas por su departamento se ajusten a los principios de protección de datos desde el diseño y por defecto.

4. Deberá especialmente velar por que se reduzca al máximo el tratamiento de datos personales en su departamento y que sea tenido en cuenta el derecho a la protección de datos en el desarrollo, diseño, contratación, configuración o uso de productos, servicios y aplicaciones que estén basados en el tratamiento de datos personales o que traten datos personales para cumplir su función.

5. Los trabajadores deberán acceder únicamente a aquellos datos que le sean imprescindibles para el desempeño de sus tareas.

6. Podrá solicitar el asesoramiento del Responsable de Privacidad para evaluar el cumplimiento del principio de privacidad por diseño y por defecto.

7. Garantizará que su departamento proporcione al Responsable de Privacidad, en el tiempo y en la forma oportuna, el soporte que este precise para el desempeño de sus funciones.

8. Las actividades de tratamiento de datos que hayan sido evaluadas como de alto riesgo, deberán ser formalmente autorizada por el órgano de administración

DECÁLOGO PARA EL DEPARTAMENTO DE RRHH

Además del decálogo RGPD general, el departamento de RRHH deberá cumplir las siguientes normas respecto al tratamiento de datos personales:

1. Los integrantes del departamento de RRHH deben conocer y aplicar el procedimiento de Aceptación de Normas y Políticas para garantizar la aceptación formal de las políticas y normas de privacidad por parte de los trabajadores, personas en prácticas o personal contratado a través de E.T.T.
2. A tal efecto, se responsabilizarán de que dichas personas firmen la correspondiente política de privacidad en el momento de su alta, archivándose la misma en su expediente.
3. A todas estas personas, se les entregará igualmente una copia de las políticas y normas de privacidad y se les informará sobre los mecanismos o canales habilitados por la organización para dar a conocer el soporte organizativo y las funciones definidas para aplicar y controlar el cumplimiento de las políticas, normas y procedimientos definidos en materia de privacidad.
4. Los expedientes de los/las trabajadores/as se conservarán en archivo cerrado bajo llave, que permitirá el acceso únicamente al personal autorizado.
5. En el caso de que a un trabajador le deban ser practicadas las retenciones sindicales en nómina, deberá solicitarlo por escrito. Dicho documento se archivará en su expediente laboral.
6. Los datos de trabajadores/as relativos a datos de salud, serán de acceso restringido al personal autorizado.
7. No podrán comunicarse curriculums a terceros, sin el consentimiento de los interesados. En caso de duda, consultar con el responsable de privacidad de la entidad.
8. Sólo se conservarán los curriculums correspondientes a perfiles que interesan.
9. A los/as candidatos/as cuyo curriculum, bien haya sido recibido directamente por email, correo o fax, o de portales de empleo para participar en un proceso de selección concreto, se les remitirá una comunicación que incluirá la cláusula informativa prevista por la organización.
10. A los/as candidatos/as que se convoquen para una entrevista se les hará firmar la política de privacidad para candidatos a un puesto de trabajo
11. Los curriculums se conservarán 1 año desde su última actualización. Transcurrido ese tiempo se cancelarán.
12. No se incorporarán a tratamientos automatizados los datos de salud que incidentalmente pueda haber comunicado un candidato, salvo los datos relativos a la eventual existencia de una minusvalía, y en su caso el correspondiente grado recogidos para el cumplimiento del deber impuesto por el Art. 38.1 Ley 13/1982 de 7 de abril, de integración social de los minusválidos.

DECÁLOGO PARA SISTEMAS

Además de las normas vigentes para el conjunto de trabajadores/as, el personal de sistemas deberá cumplir las siguientes normas respecto al tratamiento de datos personales:

1. Pruebas con datos reales:

   - La realización de pruebas con datos reales requerirá de la autorización previa del Responsable de Privacidad.
   - La realización de pruebas con datos reales atenderá a lo previsto en el procedimiento definido a tal efecto.
   - En todo caso, con carácter previo al inicio de la prueba deberá realizarse una copia de seguridad del sistema afectado.
   - En el registro de incidencias, se harán constar las pruebas realizadas, indicando los datos relativos a la correspondiente autorización y a la copia de seguridad, la persona que ejecutó el proceso y los sistemas afectados.

2. Recuperación a partir de copias de seguridad:

   - La recuperación del sistema deberá ser autorizada por el Responsable de Privacidad.
   - La realización recuperación a partir de copias de seguridad atenderá a lo previsto en el procedimiento definido a tal efecto.
   - En el registro de incidencias, se harán constar los procedimientos de recuperación de datos realizados, indicando los datos relativos a la correspondiente autorización, la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

3. Gestión de soportes de seguridad:

   - Cuando no estén en uso, los soportes de seguridad se guardarán bajo llave.
   - Mientras no estén bajo llave, los soportes de seguridad serán custodiados por la persona que se encuentre al cargo de los mismos.
   - La salida de los soportes de seguridad de las instalaciones, deberá ser autorizada por el Responsable de Privacidad, debiendo éste registrar la correspondiente autorización, utilizando a tal efecto el registro de autorizaciones para la salida de soportes y documentos.
   - La entrada y salida de los soportes de seguridad de las instalaciones, se registrará utilizando el registro de entrada y salida de soportes y documentos.
   - Durante el transporte de los soportes, la persona que se encuentre al cargo de los mismos será la responsable de adoptar las medidas necesarias para evitar la pérdida, sustracción o el acceso no autorizado a la información, utilizando a tal efecto el medio más apropiado en función del tipo y número de soportes afectados (maletín cerrado, caja precintada, etc.).
   - En caso de reutilizar soportes de seguridad, deberá realizarse un formateo a bajo nivel con carácter previo.

4. Para el desecho de equipos y soportes se adoptarán las medidas oportunas para evitar que se pueda recuperar la información (formateo a bajo nivel del disco duro del equipo, destrucción física manual de los soportes físicos: CD-ROM, DVD, cintas de seguridad, etc.).

5. El departamento de sistemas informará inmediatamente y apoyará al Responsable de Privacidad sobre cualquier brecha de seguridad, así como la evolución de la misma y de las actuaciones mitigadoras que se determinen.

DECÁLOGO PARA USUARIOS DE DISPOSITIVOS PORTÁTILES

Además del decálogo RGPD general, los/as usuarios/as de equipos portátiles, tales como ordenadores, tablets o smartphones deberán cumplir las siguientes NORMAS DE SEGURIDAD:

1. La conexión a los sistemas de la organización o el tratamiento de datos de la misma solo pueden realizarse utilizando los dispositivos portátiles proporcionados y/o autorizados por la organización.

2. El usuario es el único responsable de adoptar las medidas necesarias para evitar la pérdida, sustracción o el acceso no autorizado a su equipo. El robo o la pérdida del equipo será considerado como una incidencia de seguridad que deberá ser inmediatamente notificada al Responsable de seguridad de la organización.

3. El usuario adoptará en todo caso las siguientes medidas:

   - Deberá proteger el acceso al equipo mediante una contraseña.
   - Se activará el salvapantalla, el cual será protegido por contraseña.
   - No deberá conectarse a sistemas de la organización desde redes wifi abiertas.
   - Siempre deberán cerrarse las sesiones de todos los servicios a los que haya accedido desde su navegador.
   - No se guardará ninguna clave de acceso a recursos de la Organización en el equipo. En particular no se utilizará la funcionalidad de «Guardar contraseña» que ofrecen ciertos navegadores y sistemas operativos para registrar las credenciales para acceder a sistemas de la organización.
   - No se conectarán llaves USB o tarjetas de memoria procedentes de fuentes desconocidas sin haber controlado el contenido de las mismas con un programa antivirus actualizado.
   - Deberán activarse las opciones de cifrado del equipo propuestas por el sistema operativo.
   - Se deshabilitará la opción de sincronización de correos electrónicos de la organización con cuentas en cloud de terceros (Apple, Google, Microsoft, Dropbox, etc.)

4. Salvo autorización específica, no se podrá almacenar información de la organización en la memoria del equipo. De contar con la correspondiente autorización el usuario deberá cumplir con las siguientes medidas:

   - No podrá instalar programas o productos informáticos en el equipo sin la autorización del responsable de seguridad.

   - Las aplicaciones necesarias para el desempeño de su trabajo serán instaladas exclusivamente por los administradores del sistema.

   - Deberá hacer uso de un antivirus y firewall actualizado.

   - Deberán seguirse las pautas determinadas por la organización para la realización de la copia de seguridad del contenido del equipo.

5. Si no dispone de los conocimientos técnicos suficientes para implementar las medidas recogidas en el presente documento, el usuario deberá solicitar el soporte del departamento de Sistemas.

POLÍTICAS Y NORMAS DE PRIVACIDAD

Última actualización: Mayo 2018

DECÁLOGO PARA PERSONAS CON PODER PARA CONTRATAR SERVICIOS

Además del decálogo RGPD general, las personas de la organización que pueden contratar servicios deberá cumplir las siguientes normas respecto al tratamiento de datos personales:

1. Ud. debe conocer y aplicar el procedimiento definido por la organización para gestionar los procesos de contratación de servicios con el objetivo de garantizar que se produce de conformidad con lo previsto con el RGPD (Normas de Contratación).

2. La contratación de un servicio que suponga que el proveedor del mismo deba o pueda acceder a los sistemas de información, documentos o archivos de la organización, debe cumplir con una serie de formalismos.

3. En menor medida, pero igualmente afectados, se hallan todos aquellos servicios que supongan acceso físico a las instalaciones, aunque no requieran acceso a información o archivo alguno.

4. A modo de ilustración, se enumeran algunos ejemplos de servicios afectados por la normativa de protección de datos:

   - Servicios relacionados con el marketing (captación de clientes potenciales, realización de campañas de marketing directo, realización de perfiles de consumidores, etc.).
   - Servicios que implican gestiones relativas a datos de salud.
   - Formaciones externas.
   - Apoyo en la selección de personal.
   - Servicios de gestorías, asesorías y consultoras.
   - Servicios tecnológicos y de comunicación, housing.
   - Servicios webs (hosting, administración de webs, etc.).
   - Video-vigilancia y control de acceso.
   - Custodia y destrucción de archivos.
   - Colaboraciones relativas a clubs de fidelización, tarjetas de pago o de crédito, etc.
   - Limpieza.
   - Mantenimiento de instalaciones.

5. Ud. debe igualmente conocer y aplicar el procedimiento de Aceptación de Normas y Políticas para garantizar la aceptación formal de las políticas y normas de privacidad por parte de aquellos colaboradores o usuarios externos con acceso a sistemas de información, documentos o archivos de la organización.

6. En caso de duda sobre el servicio que se plantea contratar, deberá obligatoriamente consultarse al Responsable de Privacidad.