GISELLA GRUBER: Vamos a comenzar este seminario web en apenas unos minutos. Todavía se están conectando algunos participantes. El audio en Adobe Connect será en idioma inglés. Si desean unirse a los canales en español o francés, por favor, me envían un mensaje a través del chat para que los podamos conectar. Gracias.

Tijani, vamos a comenzar con la grabación y la interpretación simultánea de esta sesión. Buenos días, buenas tardes y buenas noches a todos. Bienvenidos al primer seminario web del ciclo 2018 de creación de capacidades de At-Large. En el día de hoy hablaremos acerca de protección de datos, qué necesitamos saber como usuarios finales acerca del GDPR. Este seminario web se realiza el 24 de enero de 2018 a las 13:00 UTC. No vamos a verificar la asistencia porque este es un seminario web. Contamos con interpretación a los idiomas español y francés. Les recuerdo que por favor digan su nombre al tomar la palabra para que los intérpretes los puedan identificar en cada uno de los canales de idiomas y también para tener una transcripción adecuada.

Por favor, si están en Adobe Connect y también conectados telefónicamente, les pido que silencien sus teléfonos y sus computadoras cuando no estén tomando la palabra. Con *6 se silencia su línea y la vuelven a habilitar con *7. Por último, por favor, hablen a un ritmo que sea lo suficientemente pausado como para permitir una interpretación adecuada. Dicho esto, le doy la palabra a Tijani.

TIJANI BEN JEMAA: Muchas gracias, Gisella. Bienvenidos a todos. Buenos días, buenas tardes y buenas noches. Desde mi punto de vista, hoy tenemos uno de los seminarios web más interesantes porque vamos a hablar acerca de un tema que afecta a la comunidad de la ICANN y a la comunidad de Internet en general. Tiene que ver con el futuro del DNS en cierto modo. Incluso si no somos un registrador o un registro y si no estamos ubicados en Europa o aunque no tengamos una empresa en Europa podemos vernos afectados por este nuevo reglamento, el GDPR, que afectará al tratamiento de datos en Europa. Creo que este es un tema muy importante. Es de suma importancia porque tenemos un tiempo muy acotado para poder estar al tanto y listos para este GDPR. Vamos a seguir tratando este tema en la ICANN.

En el día de hoy contamos con dos oradores muy importantes. Thomas Rickert, que es uno de los presidentes del CCWG sobre responsabilidad. Por supuesto, desempeña muchos otros roles pero quiero recalcar este rol en particular porque él lo desempeña sumamente bien. También contamos con Chuck. Todos conocen a Chuck. Él está en el grupo de trabajo de la próxima generación de RDS. Él ya nos ha brindado muy buenas presentaciones. Dicho esto, Les doy la palabra a los miembros del personal. Luego ya pasaremos a las presentaciones. Gisella, tiene la palabra.

GISELLA GRUBER: Muchas gracias, Tijani. Para quienes están en el Adobe Connect, por favor, lean la diapositiva que está en pantalla. Voy a comenzar ahora a explicar el procedimiento. Para publicar preguntas tienen un sitio

específico en el Adobe Connect. Estas van a ser enviadas a los presentadores. Tengan presente también que vamos a tener algunas preguntas, un cuestionario, después de las presentaciones. Estas preguntas van a estar en la sala de Adobe Connect. Quienes están en la sala de Adobe Connect tienen que estar listos para participar y contestar estas preguntas utilizando la herramienta correspondiente. Después del seminario web vamos a hacer una encuesta para ver su experiencia como usuarios. Esta encuesta tendrá siete preguntas. Les agradecemos que por favor se tomen alrededor de cinco minutos para completar esta encuesta porque es realmente muy importante recibir sus comentarios acerca de estas iniciativas de creación de capacidades.

TIJANI BEN JEMAA: Muchas gracias, Gisella. Muy bien. Nuestro primer orador será Thomas Rickert, quien hablará acerca del GDPR en rasgos generales. Luego nos dirá cómo impacta nuestro trabajo en la ICANN. Luego Chuck nos hablará acerca del grupo de trabajo en el cual él está en este momento, del trabajo que están realizando, qué es lo que están haciendo en este momento para poder cumplir con esta normativa. Tiene la palabra Thomas.

THOMAS RICKERT: Muchas gracias, Tijani. Muchas gracias, Gisella, Heidi, Silvia, por esta invitación. Quiero darles la bienvenida a todos ustedes a este seminario web sobre un tema que es muy importante y espero que también sea interesante. Quiero pedirles disculpas a Camila, Sabrina, Claudia, Jacques, a los intérpretes a los idiomas español y francés porque

probablemente sea un tanto difícil volcar todo este vocabulario jurídico a sus respectivos idiomas. También quiero decirles que me complace mucho ser el primer orador porque hablar después de Chuck Gomes es realmente un desafío.

Ahora vamos a entrar de lleno en esta presentación. Van a ver que tenemos muchas diapositivas pero no se asusten porque tenemos muchos gráficos en esta presentación. Lo que yo quería era dejarles este material como referencia y futura lectura para que puedan digerir con mayor facilidad toda esta información que les voy a presentar en estos próximos minutos. Muy bien.

El GDPR es un tema muy amplio. No esperen transformarse en expertos en el GDPR en este tiempo tan acotado. Lo que queremos lograr, y lo hablé con Tijani, es lo siguiente. Quiero presentar los conceptos generales del reglamento europeo sobre la protección de datos y ver algunos aspectos específicos para la industria de nombres de dominio y para los usuarios finales. Seguramente vamos a ver cambios importantes en la industria de nombres de dominio y también seguramente habrá debates muy apasionados en los próximos meses, en las próximas semanas. Espero que ustedes puedan comprender de qué se tratan todos estos debates y que puedan participar en los debates teniendo una postura con mayor información después de haber escuchado nuestras presentaciones.

Yo represento a la asociación ECO. Es una asociación de la industria de Internet con sede en Alemania con más de mil miembros de más 60 países. Nosotros nos encargamos de administrar el punto de

intercambio de Internet [DE-CIX]. Nosotros nos encargamos de cuestiones de la industria de nombres de dominio. Tenemos más de 150 países que trabajan con nosotros y nosotros también gestionamos más del 60% de los nombres de dominio a nivel mundial.

Muy bien. Este reglamento, el GDPR, no es un algo nuevo. Se viene tratando desde hace muchos años pero fue aprobado y publicado hace aproximadamente dos años. Es decir, hubo un plazo de dos años antes de su entrada en vigencia. Todos dicen que esto es algo muy nuevo pero en realidad ya es aplicable. Lo que pasa es que el 25 de mayo de 2018 entrará en vigencia.

También hay un mito que debemos aclarar. Quienes conocen cómo se realiza la legislación en Europa habrán escuchado hablar de la palabra directriz. Esta directriz debe pasar al estatus de legislación nacional. Hasta tanto se haya llegado a ese paso, esta directriz no será aplicable en los distintos mercados europeos. Un reglamento es aplicable a todos los estados miembros y a todos los estados que están regidos por el GDPR.

Muy bien. Este reglamento tiene por objetivo regular la protección de datos de manera uniforme en la Unión Europea para que sus ciudadanos puedan controlar mejor sus datos personales y regular cómo los encargados del tratamiento de datos pueden usar sus datos personales. También quiere asegurar el libre flujo de los datos personales dentro de la Unión Europea y regular la exportación de datos personales fuera de la Unión Europea.

Este reglamento se ocupa de los datos personales, no de otro tipo de datos. Ahora bien, ¿qué son los datos personales? Son datos que permiten identificar a las personas. Según nuestra resolución de la Corte Suprema, incluso una dirección de IP puede ser un dato personal porque alguien puede ver quién es el titular de esa dirección IP en algún momento determinado.

Estos datos van más allá de la dirección de un individuo. Con lo cual, los nombres de dominio pueden ser datos personales si permiten que se pueda identificar a un titular de datos. También un número telefónico, una dirección de correo electrónico, un número de fax. Todos esos datos son datos personales. Esto se aplica a la Unión Europea.

También en la pantalla vemos que se quiere facilitar el flujo libre de datos personales dentro de la Unión Europea pero hay un desafío mayor que implica la exportación de datos fuera de la Unión Europea. En el futuro, si un registro o registrador quiere divulgar datos a quien le pida esos datos, se va a tener que verificar que ese principio de divulgación sea legítimo y también verificar de dónde proviene esa solicitud de datos. También va a tener que asegurarse de que esa exportación de datos personales sea legítima.

Este reglamento implica mayores requisitos en cuanto a transparencia. Es decir, hay que documentar lo que se hace con estos datos. Hay que informar a los titulares de los datos acerca de las actividades que se realizan con esos datos. Hay que tener un registro de actividades de procesamiento de datos y también hay que demostrar que el titular de

datos brindó su consentimiento dentro de un sistema utilizado para obtener los datos personales.

Luego también hay requisitos en cuanto a la seguridad de los datos, mayores requisitos también en cuanto a rendición de cuentas y responsabilidad y también la obligación de informar las violaciones a la seguridad de los datos personales. Por ejemplo, si datos que no se pueden divulgar son entregados o compartidos ampliamente, eso puede constituir una violación a la seguridad de los datos personales, puede afectar la integridad de esos datos y esas instancias pueden ser internas o externas. Por ejemplo, un empleado puede cometer un error. Hay que ver qué sucede en ese caso y hay que ver si hay que informar esa instancia a la autoridad supervisora correspondiente.

También hay ciertos plazos. Hay que remediar estos errores con celeridad. Vemos que los legisladores se toman esto muy en serio y quieren asegurarse de que nadie pueda esconder o mantener en secreto estas violaciones a la seguridad de los datos personales. Luego también está el derecho al olvido si uno no quiere estar más en una plataforma de red social, por ejemplo. También hay algunas obligaciones de un operador de datos que tiene que mantener esos datos durante un tiempo por cuestiones de requisitos legales. También está el derecho a la portabilidad de datos. Si ustedes están con la empresa A hoy en día y quieren cambiarse a la empresa B, tienen que tener la posibilidad de llevarse sus datos con ustedes.

También hay otros conceptos. Privacidad por defecto y por diseño. La privacidad por defecto indica que una configuración de un entorno

determinado debe ser muy estricta desde el principio de manera tal que si un cliente va a una plataforma en una red social puede, si lo desea, cambiar esa configuración para que no sea tan estricta pero desde el diseño, desde el [inaudible], la configuración tiene que ser muy estricta.

La privacidad por diseño significa que hay que diseñar un sistema de manera tal que no pueda obtener y recolectar más información personal de lo necesario. Por ejemplo, en un software determinado hay que asegurarse de que el programa correspondiente siga el principio de minimización de datos.

Ahora vamos a ver algunos principios de la licitud del tratamiento de datos. Esto lo vamos a seguir tratando durante nuestra conversación en el día de hoy. Esto se basa en el artículo 6 del GDPR. El tratamiento de datos será lícito solamente… A ver, perdón, voy a retroceder en la presentación. Aquí. Bien.

El procesamiento será lícito solamente si se cumple al menos uno de los siguientes principios. Primero, consentimiento. El principio de consentimiento. Luego, si hay que procesar los datos para poder realizar o ejecutar un contrato. Licitud de tratamiento para cumplir con una obligación legal. Por ejemplo, si yo soy un registro o registrador y tengo una obligación legal de procesar los datos de una determinada manera, no necesito el consentimiento explícito del titular de los datos. Luego, el procesamiento de los datos debe ser necesario para proteger los intereses vitales del titular de los datos. Luego también está el principio de procesamiento de datos en pos del interés público o en el ejercicio de la autoridad oficial del encargado del tratamiento de los datos. También

intereses legítimos por parte del encargado del tratamiento de los datos o un tercero excepto cuando estos intereses queden supeditados a los intereses o derechos fundamentales y libertades fundamentales del titular de los datos, sobre todo cuando se trata de proteger datos personales, especialmente si el titular de los datos es un niño.

Muy bien. Los principios A, B y F van a ser los más importantes. El consentimiento, el procesamiento de datos para la ejecución de un contrato y luego el procesamiento de datos en respuesta a intereses legítimos. Con respecto al aspecto contractual, si uno vende libros por Internet, por ejemplo, no necesita permiso adicional del cliente para solicitarle al cliente la dirección a la cual enviarles los libros. Uno necesita esa dirección porque si no, no puede cumplir su contrato con el cliente. Hay mucha confusión alrededor de esa cláusula en particular. Por eso la traigo a colación, porque siempre tenemos que tener en cuenta la relación contractual entre el cliente o titular de los datos y el operador. Siempre vamos a ver la relación contractual entre el revendedor y el registratario o el registrador y el registratario. Tenemos que ver el acuerdo de acreditación de registradores con la ICANN y tenemos que ver su licitud para el procesamiento de datos. Tengan esto presente. Seguramente van a escuchar mucho más al respecto en el futuro cercano.

Muy bien. Pasemos al consentimiento. Actualmente en el sistema de nombres de dominio para los gTLD, en el acuerdo de acreditación de registradores se indica que se debe obtener el consentimiento del titular de los datos pero esto tiene un problema porque el encargado de controlar y procesar los datos tiene que demostrar el consentimiento del

titular de los datos y el titular de los datos, sin motivo alguno, puede retirar su consentimiento. Si ustedes basan el procesamiento de datos en el consentimiento y luego el titular de los datos retira ese consentimiento, están en problemas.

También el consentimiento se debe prestar libremente. Los registradores o revendedores dicen: “Sí. Usted puede tener ese nombre de dominio genérico pero solamente si nos da el consentimiento para que sus datos sean públicos”. Por ejemplo, desde el punto de vista legal, y esto lo digo sobre la base de información que hemos obtenido del grupo que se encarga de la protección de datos personales en Europa, ese grupo dijo que eso va en contra de la prohibición de acumulación del consentimiento. Tenemos que tenerlo en cuenta para la administración de nombres de dominio.

Luego tenemos que ver a quién se aplica esto. Uno podría decir: “Yo estoy fuera de la Unión Europea, entonces a mí esto no me afecta, el GDPR”, pero sí los va a afectar porque el GDPR se aplica no solo a los encargados de procesar datos dentro de la Unión Europea sino también a quienes procesan datos de titulares de datos de la Unión Europea. Si ustedes tienen clientes que son ciudadanos de la Unión Europea, aunque ustedes estén fuera de la Unión Europea ocasionalmente el GDPR será aplicable para ustedes también. Con lo cual, necesitan un representante dentro de la Unión Europea para que pueda responder a solicitudes de información de los titulares de datos y también para que se pueda comunicar con las autoridades pertinentes.

Con respecto a las sanciones, se ha hablado mucho acerca de las sanciones en el marco del GDPR. Hay regímenes de protección de datos muy estrictos en Europa donde se vienen aplicando estas ideas desde hace mucho tiempo. Las autoridades de supervisión lo que hicieron fue ver cuáles eran las empresas que no cumplían con las leyes de protección de datos. Ahora, con este GDPR, vamos a ver multas para cuestiones menores que pueden llegar hasta 10 millones de euros y el 2% de los ingresos anuales. Para casos severos tenemos multas de hasta 20 millones de euros y hasta el 4% de los ingresos anuales de una compañía. Eso afecta a quienes trabajan con datos personales.

También, los titulares de datos pueden tener la autoridad de actuar en caso de que no actúen las autoridades. El usuario tiene el poder a través de los grupos de usuarios de informar estas situaciones, de tomar esto seriamente y de que se actúe en consecuencia.

¿Qué implica esto para la ICANN y el mundo de los gTLD? La ICANN está en una situación difícil porque Fadi Chehadé, que todos ustedes recordarán como director ejecutivo de la ICANN, en uno de sus discursos inaugurales en una reunión de la ICANN dijo que había dos cuestiones en el mundo que no se podían resolver: el conflicto palestino y WHOIS. Yo no hubiera elegido esos ejemplos pero definitivamente demuestran la complejidad del debate en materia de WHOIS. Por una parte están quienes tienen un gran interés en que los datos estén disponibles. Por ejemplo, los organismos de cumplimiento de la ley y del orden público. Y hay personas que quieren saber con quiénes están haciendo negocios en Internet. Por otra parte están quienes defienden la protección de datos. Tenemos que reconciliar estas dos posturas.

La ICANN obviamente tiene que hablar acerca de esto con los registros y los registradores y tiene que cumplir las normas aplicables. Esto es una prioridad principal. En este nuevo sistema, quienes controlan y procesan los datos enfrentan el riesgo de sanciones, de multas. Las empresas que utilizan el DNS, ellos no corren el riesgo de ser multados. Hay que lograr un cumplimiento contractual y esto es importante para la ICANN.

En Abu Dabi se anunció que la ICANN abordaría esto en dos etapas. Primero, la etapa de cumplimiento contractual para ver cuáles son las empresas que no cumplen con los acuerdos de registro y registrador para que no corran el riesgo de recibir notificaciones de incumplimiento por parte de la ICANN. Luego, a largo plazo, habrá un proceso de la comunidad dentro del modelo de múltiples partes interesadas y de la creación de políticas correspondiente.

En los últimos días, la ICANN publicó tres modelos y solicitó comentarios de la comunidad sobre estos modelos y hay tiempo para presentar comentarios hasta el 29 de enero. Vamos a hablar en más detalle acerca de estos modelos en esta presentación.

Como yo soy abogado y trabajo en el espacio del DNS participo mucho en estos temas, en estos debates. Nosotros presentamos un modelo a la ICANN para su revisión, para que pueda ser utilizado como modelo de cumplimiento, por lo menos para esta primera etapa inicial. Vamos a ver parte del material que utilizamos para presentar este modelo. Alguna de las ideas no van a ser aceptadas de manera universal porque son controvertidas pero creo que aportan valor en cuanto a que facilitan la comprensión de esta cuestión tan compleja.

Los modelos propuestos por la ICANN se centran en la divulgación de datos principalmente. Todo el mundo habla del WHOIS respecto del GDPR pero hay que ver todo el proceso mediante el cual se obtienen los datos. Como dije anteriormente, hay principios de licitud del tratamiento de datos y hay que comprender los fundamentos legales de cada paso del proceso, desde que se obtienen los datos hasta que se modifican los datos y también teniendo en cuenta su transferencia a terceros y su eliminación. También hay que ver si los datos son públicos o semipúblicos en WHOIS. El modelo que propone la ICANN se centra solo en la parte de la divulgación.

La ICANN también supone que con estos modelos se pueden recabar todos los elementos de datos disponibles pero eso es problemático debido al principio de minimización de datos que mencioné. Hay que ver si realmente necesitamos los datos y si hay que recabarlos para cumplir con las políticas y los contratos de la ICANN. También suponen que los datos pueden viajar fácilmente del registrador al registro y esto también es algo que hay que mirar más de cerca.

Vamos a ver cuáles son las partes implicadas en el procesamiento de datos en el sistema de los gTLD. Vemos a los usuarios de Internet que van a un registrador, ingresan datos o bien van a un registrador acreditado y ese registrador puede tener un acuerdo con un revendedor. El registrador tiene un acuerdo con los registros y ambos tienen sus agentes de custodia de datos a los cuales transfieren los datos. Luego tenemos el [inaudible], el operador de registro back end de emergencia, que entra en juego cuando un registro no puede funcionar. Entonces la ICANN puede pedirle al registro que le pase los datos y luego pasar esos

datos al [inaudible]. Creo que esa es la manera en la que se puede realizar. También, este [inaudible] actúa como agente de custodia de datos. La ICANN tiene relaciones contractuales con registros, registradores y con estos registros de emergencia [inaudible].

Tenemos clientes de WHOIS que quieren acceder a datos a nivel de registro o registrador. Lo que tratamos de hacer es confeccionar un modelo que tenga en cuenta los riesgos legales que implica el procesamiento de datos. Tenemos las disposiciones 6.1.A, 6.1.B y 6.1.F, consentimiento, ejecución de un contrato y actuar en pos de intereses legítimos.

Podemos asignarles niveles de riesgo a cada una de estas categorías. En el primer nivel tenemos la ejecución de un contrato. Uno necesita vincular un nombre de dominio a un registratario para asegurarse de que ese registratario sea el titular de ese nombre. En el nivel intermedio tenemos los intereses legítimos. Por ejemplo, si yo quiero procesar los datos necesito averiguar, por ejemplo, si hay conductas ilegales en mi base de registratarios por cuestiones de seguridad. Bueno, ese puede ser un interés legítimo pero el cliente, el titular de los datos puede decir que sus derechos están en conflicto con mis intereses legítimos. Hay que llegar a un término medio y hay que reconciliar el interés legítimo con los derechos del titular de los datos. Si uno tiene el derecho de procesar los datos, puede seguir adelante pero puede recibir objeciones. Luego, el mayor nivel de riesgo es el del consentimiento porque existe el riesgo de que el cliente retire su consentimiento y eso va a generar un problema porque ya no podemos procesar los datos.

Los datos recolectados pueden ir a distintos lugares. Tenemos los datos administrativos C, técnicos C, de facturación C. Luego tenemos datos de registratarios, datos que indican quién es el registro, el registrador. Algunos datos que sirven para especificaciones. Luego datos de los titulares de las cuentas.

Para nosotros, hace falta diferenciar distintos escenarios de registros. Si un registro no tiene requisitos específicos, eso equivale a .COM, por ejemplo. Es un nombre genérico de alto nivel abierto. Pero, por ejemplo, luego tenemos a nexus. Para tener un nombre en .BANK, uno debe ser una entidad bancaria. Luego hay que hacer una validación para ver si el registratario es un registratario legítimo. El registro puede solicitar datos para cumplir con su contrato. Por ejemplo, .BANK puede pedirles todos los datos necesarios al registrador porque tiene que validar al cliente. Si no existen esos requisitos, es posible obtener los datos del registrador si se puede invocar un interés legítimo por parte del registro.

Tenemos que ver qué hace falta para llevar adelante un contrato, para la ejecución de un contrato. Los cuadros en color rojo, administrativo C, técnico C y facturación C, ya no son necesarios si uno tiene en cuenta el principio de minimización de datos. Necesitamos los datos del registratario pero ya no necesitamos el resto de los datos. Podemos ir al titular de la cuenta para solicitar más datos. El registrador le manda la factura al titular de la cuenta y no se va a fijar en el contacto de facturación en el sistema de WHOIS.

Según el principio de minimización de datos tendríamos al registrador, que recolecta los datos del registratario. Luego tendríamos datos

técnicos que también son recolectados y solamente se transfieren al registro los datos del nombre de dominio y no el resto. Si el registro invoca un interés especial, lo puede hacer. Puede obtener esos datos pero eso debe quedar especificado en los acuerdos de registro, en el acuerdo de acreditación de registradores también, y la ICANN no debería forzar el procesamiento basado en el consentimiento porque eso es algo bastante riesgoso.

Nosotros tenemos aquí en este modelo a los registradores, a los registros y a la ICANN que según el punto de vista del estudio jurídico a cargo de este análisis serían en conjunto quienes controlan los datos. Luego tenemos a los agentes de custodia de datos y al registro de emergencia [inaudible].

Con esto les quiero mostrar que para la ICANN es importante que registros y registradores se comuniquen entre sí porque de acuerdo a la nueva legislación uno tiene que poder decirle al cliente exactamente quién hace qué cosa, qué responsabilidad tiene cada una de las partes involucradas. Con lo cual, hay que establecer muy claramente las responsabilidades. Bien, ya hablé acerca del modelo básico. ¿Puede el registrador agregar elementos de datos? Sí, puede. ¿Puede hacerlo el registro? Sí, también puede pero solamente un conjunto básico de datos para llevar adelante su contrato. Esto es lo que tendría que exigir la ICANN. Tenemos el requisito de vínculo o nexo, poder ser elegible. Luego los datos administrativos C también se podrían recolectar, que no se podría hacer según el contrato.

Pasemos ahora a la divulgación de información. Este es un tema muy difícil porque uno no puede automáticamente divulgar todos los datos que puede recolectar de manera lícita. Definitivamente, a partir del 25 de mayo la información no se va a poder publicar como se publica hoy porque no tenemos un fundamento jurídico para esa publicación amplia de los datos. Eso está en consonancia con el grupo del artículo 29 que protege los datos.

Tenemos que ver el tema del acceso protegido o restringido a WHOIS. Si uno está certificado para solicitar la información, entonces puede acceder a esa información. Hay que ver que se use el servicio solo para unos fines específicos y puede haber distintas categorías de usuarios que estén certificados para solicitar información.

Luego, respecto de los servicios de privacidad y representación o proxy, estos deberían seguir en pie y luego tenemos distintas instancias de divulgación que se pueden fundamentar en la ejecución de un contrato, el UDRP y el URS, por ejemplo. Uno puede recurrir a estas políticas para impugnar un registro de un nombre de dominio. Tiene que verificar si el registratario es legítimo. Eso se puede demostrar solo accediendo a los datos. En estos casos hay que permitir el acceso a los datos.

Luego, respecto del artículo 6.1.C, el cumplimiento de obligaciones legales, si uno tiene que cumplir con pedidos de organismos de cumplimiento de la ley tiene que obtener los datos pero esto tiene que ver con entidades europeas en el cumplimiento de la ley. Aquí vemos un nuevo diagrama. Tenemos los organismos de cumplimiento de la ley europeos y los que no son europeos. Estos últimos deberían tener un

acuerdo de asistencia mutua para poder acceder a estos datos. Esto afecta a los organismos de cumplimiento de la ley a nivel mundial y consideramos que los legisladores deben garantizar las herramientas adecuadas para estos participantes. Sin estas herramientas, y creo que los legisladores se olvidaron de incluir esto porque pensaron que el WHOIS estaría abierto por siempre, los registros y registradores corren el riesgo de procesar datos de manera que no sea lícita.

Voy a ir cerrando ahora mi presentación. El WHOIS sería cerrado. Uno puede escribirle al registrador para que se comunique con el registratario pero no hay acceso directo a los datos. Luego tenemos un programa de certificación para que determinadas personas puedan acceder al segundo nivel de WHOIS y también va a haber que presentar solicitudes individuales que podrán ser analizadas para facilitar este proceso para poder gestionar estas solicitudes de divulgación de información. Esto se puede hacer sobre la base del protocolo de WHOIS y de la medida que lo remplace. Vamos a tener autoridades de certificación que otorguen acceso a las distintas partes. Les dejo todo este material para que sigan leyendo. Yo les acabo de dar una reseña y ahora voy a concluir mi presentación. Gracias por su atención.

TIJANI BEN JEMAA: Muchísimas gracias por la presentación. Ahora le voy a ceder la palabra a Chuck, quien nos va a hablar del trabajo que están haciendo en el grupo de trabajo, sobre todo el trabajo que están haciendo para darle cumplimiento al GDPR.

CHUCK GOMES: Gracias, Tijani. Gracias por la invitación. Les agradezco la oportunidad para poder hablar de cuál es la relación con el PDP de servicios de directorio de registración para la próxima generación. Voy a ser relativamente breve porque no soy un experto en GDPR. Le agradezco realmente a Thomas el elogio que dio en su presentación. Voy a agradecer realmente y a felicitar a Thomas porque hizo un excelente trabajo en poco tiempo. Vamos a ir ahora a lo que es el casillero número dos.

Yo me voy a concentrar entonces en cuál es la relación entre el GDPR y el proceso de desarrollo de políticas del RDS. Brevemente voy a hablar de cuál es el objetivo que tiene este PDP. Les voy a dar una idea general de cuál es el estado de situación y después vamos a hablar de cómo ese PDP tiene relación con el GDPR.

Vamos ahora a la imagen número tres donde tenemos el objetivo de este PDP. Nosotros tenemos que definir el objetivo de recabar, mantener y brindar acceso a los datos de registración de los gTLD considerando las medidas de protección para precisamente proteger esos datos. Eso tiene que ver obviamente con proteger los datos, según dice el GDPR, en Europa y también en otras partes del mundo que tienen trato con Europa.

La GNSO le da una carta orgánica a cada uno de sus grupos de trabajo, sobre todo los que tienen a su cargo un PDP, y querría señalar que existen tres fases en nuestro trabajo y pueden verlas ustedes en el centro del flujograma. La primera fase, en la que todavía estamos, es la de definir cuáles son los requisitos para establecer un sistema de RDS.

Una vez que hayamos definido los requisitos y hay ciertos procesos que tienen que ver con la aprobación para llegar a ese punto, después vamos a desarrollar una política para cumplir con estos requisitos. Esta sería la fase dos. En la fase tres vamos a desarrollar las guías de implementación. Obviamente, hay pasos previos y posteriores en todas estas etapas.

Una de las cosas clave que tenemos que entender, y la pregunta fundamental en la que yo me centro, es lo que está en el centro porque dice: “Tiene que ser completado”. Dice: “Si necesitamos un RDS de siguiente generación y por qué”. Esta es la pregunta fundamental que el grupo de trabajo debe responder. Si se necesita un nuevo RDS para remplazar al sistema actual, para modificarlo, para cumplir con los requisitos que desarrollemos sobre todo en lo que tiene que ver con las cinco primeras preguntas de las 11 de la fase 1. Todavía estamos ahí. Lo pueden ver en el flujograma.

Ya señalé que todavía estamos en la fase uno, en la primera parte diría yo de la fase uno, que es la más difícil porque si el grupo recomienda que se necesita un nuevos sistema RDS y nosotros completamos todos los requisitos para la fase uno, recién en ese momento vamos a pasar a la fase dos que tiene que ver con el desarrollo de la política y después la fase tres que es la implementación.

Si pasamos a la imagen número cuatro, durante la fase uno lo que tratamos de hacer en el grupo de trabajo es llegar a un consenso sobre las siguientes preguntas. Yo ya hablé de cuáles son los requisitos fundamentales y para cada una de las fases tenemos 11 preguntas o

categorías incluidas en esa carta orgánica que nos marca el trabajo que tenemos que realizar. Antes de responder la pregunta sobre los requisitos fundamentales, si se necesita un nuevo sistema o no, tenemos que agregar un mínimo, teniendo en cuenta los usuarios, los objetivos y los accesos vinculados con los datos, la exactitud de los datos, cuáles son los elementos de datos y además los requisitos de privacidad.

Obviamente, Thomas ha hecho un excelente trabajo hablando de este último punto que son los requisitos de privacidad dentro del GDPR. Sabemos que en otras jurisdicciones del mundo también existen requisitos de privacidad específicos diferentes de los del GDPR en algunos casos.

La tercera viñeta donde nos dice si necesitamos un marco de política y un RDS de siguiente generación para estos requerimientos, si la respuesta es sí vamos a tener que desarrollar requisitos que estén vinculados con estas otras áreas que tienen que ver con la coexistencia, el cumplimiento durante esta coexistencia, un modelo del sistema, el costo, los beneficios. Además, lo que es el análisis de riesgo. En esta área es cuando decidimos si se necesita este nuevo sistema.

Si decimos que no lo necesitamos, cosa que por lo que vemos resulta improbable, tenemos igualmente que responder a esta pregunta. Digamos que la respuesta es no, que no necesitamos un RDS de siguiente generación, que podemos modificar el WHOIS actual para cumplir con los requisitos.

En la imagen cinco podemos ver aquí cuáles son las distintas fechas meta que tenemos. Hubo una resolución de la junta directiva en abril del

2015. Se aprobó la carta orgánica en noviembre de ese año y dos años atrás empezamos con el grupo de trabajo. Hace dos años entonces que empezamos a trabajar. Este es el tercer año de trabajo para nosotros.

En junio de 2016 desarrollamos una lista de posibles requerimientos y en noviembre de 2016 se iniciaron las deliberaciones que no han terminado y que tienen que ver con los requisitos específicos. Nuestro objetivo ahora es que para junio de este año, de 2018, iniciemos entonces el desarrollo de un informe inicial. Va a haber un informe inicial para la parte uno pero en realidad estamos planeando tener dos, por eso ustedes pueden ver que dice: "Primer informe inicial", porque necesitamos los comentarios de la comunidad, también de la comunidad At-Large. Esto obviamente lo vamos a recibir después de haber respondido a las primeras cinco preguntas dentro de nuestra carta orgánica.

Los próximos pasos entonces son: terminar con la deliberación sobre las preguntas uno a cinco que tenemos en la carta orgánica, que son las que establecen las bases para saber si necesitamos un nuevo sistema o no. Después, como dije, esperamos que para junio de este año empecemos a preparar el primer informe inicial para recibir los comentarios que nos tenga que hacer la comunidad. Quiero decir algo. Cuando hablamos de los comentarios para el grupo, obviamente también pueden hacerlos dentro del grupo porque At-Large tiene muchos miembros que están participando en el grupo de trabajo. Obviamente recibimos los comentarios de At-Large y también de las personas en su calidad de individuos.

Después de haber publicado este primer informe inicial y recibir los comentarios vamos a modificar nuestro plan de trabajo, según resulte necesario, y suponiendo entonces que necesitamos un nuevo sistema, vamos a deliberar sobre las siguientes de la carta orgánica hasta llegar a la número 11. Vamos a producir un segundo informe inicial y después un informe final que va a recibir el consejo de la GNSO. Suponiendo que el consejo lo apruebe, vamos a pasar a las fases dos y tres. Las fases dos y tres quizá puedan ir un poco más rápido o en paralelo pero esto lo tiene que decidir el consejo. Vamos a pasar ahora a la siguiente imagen.

Yo creo que la pregunta clave es cómo el GDPR guarda relación con este PDP. En primer lugar querría decir que en la primera viñeta este es un proceso de múltiples partes interesadas ascendente que va a tomar muchos años, como ha pasado en los últimos 17 años con cualquier tema vinculado con el WHOIS. El PDP debe dar respuesta a los requisitos de protección global de datos, no solo a los que provienen de Europa. Sucede que el GDPR es un ejemplo excelente de lo que son los requisitos de privacidad y protección de datos para manejar lo que es la información personal de las personas físicas. En el grupo de trabajo nos estamos concentrando en lo que sucede en el GDPR porque realmente es un muy buen ejemplo de lo que son los requisitos de protección de datos.

El trabajo que se está haciendo ahora para cumplir con el GDPR en lo que tiene que ver con el WHOIS tal cual está hoy en el que están los registradores, ICANN, los registros, ECO, se va a utilizar en el PDP según resulte aplicable porque entonces también nos va a ahorrar tiempo para el futuro.

Es muy importante. Querría hablar de la última viñeta. Cualquier RDS de próxima generación va a ser una solución de largo plazo para manejar los requisitos de protección de datos y privacidad y el manejo de estos datos. La única forma de modificar los requisitos de datos de registración en lo que son los contratos con los registradores y los registros es esta, excepto cualquier cambio de política de emergencia que pudiera implementar la junta directiva de la ICANN.

Vamos a tratar de que en el corto plazo, como dijo Thomas, no existan estas multas porque tenemos la fecha límite del 25 de mayo. Es muy importante que surjan algunas decisiones de parte de la junta directiva para cambiar políticas pero esto no tiene que ver con el PDP porque son cambios de emergencia en la política y esto no va a predeterminar lo que sean las recomendaciones del grupo de trabajo del PDP porque el grupo de trabajo obviamente va a analizar esos cambios dentro de su proceso de desarrollo de políticas.

Esta última imagen, que es la número siete, es para agradecerles y obviamente vamos a tener ahora tiempo para preguntas y respuestas. Agradezco la oportunidad de responder a sus preguntas en este seminario. Muchísimas gracias.

TIJANI BEN JEMAA: Muchas gracias, Chuck, por la presentación. Antes de darle la palabra al personal para ver si hay preguntas, yo quería agregar y preguntarle a Chuck si nos puede explicar la diferencia entre lo que es el WHOIS amplio y el acotado porque me parece que sería bueno que la

comunidad entendiera cuál es el modelo que existe en la actualidad con este WHOIS amplio y acotado. ¿Es posible?

CHUCK GOMES: Gracias, Tijani. Muchos de ustedes saben que parte de los PDP que tienen éxito con el WHOIS tienen que ver con el WHOIS amplio. Esto fue aceptado y aprobado como política, primero por el consejo de la GNSO y después por la junta directiva de la ICANN. Esta política de consenso tiene que ver con la fase de implementación que se está dando y, si bien está demorada debido a los requisitos de privacidad y protección de datos como el GDPR, se está tratando de implementar este WHOIS amplio a los registros que todavía siguen teniendo un WHOIS acotado pero todos empezaron a darse cuenta rápidamente de que teníamos un problema transfiriendo todos estos grandes datos a los registros. Es por eso que por el momento está en pausa, si bien había gente que quería que se diera, porque hubo problemas serios.

Lo que Thomas acaba de compartir, creo que muchos de ustedes pueden ver que hay un problema con todos estos datos que masivamente se empezaron a transmitir a los registros de parte de los registradores. Ese es un problema que todavía no hemos resuelto.

Voy a compartir una opinión personal en este sentido. Yo creo que probablemente debido a que las recomendaciones del grupo de trabajo del PDP para el WHOIS amplio han sido mejoradas, estas recomendaciones van a tener que volver al grupo de trabajo, al menos esa es una opción, para que puedan analizarlas nuevamente a la luz de cosas como el GDPR.

Muy buena pregunta, Tijani, realmente, para este webinar. Puedo suponer que todos entienden cuál es la diferencia entre el amplio y el acotado dentro del WHOIS. Si no es así, por favor, háganmelo saber porque es una distinción importante. En el grupo de trabajo nosotros dejamos de usar el término WHOIS acotado y ahora decimos conjunto de datos mínimos. Para seguir trabajando dentro de ese grupo de datos públicos mínimos digamos que hemos reducido bastante lo que es esta diferencia entre el WHOIS amplio y el acotado.

TIJANI BEN JEMAA: Saben que acotado significa datos mínimos y que el WHOIS amplio significa todos los datos cuando uno adquiere un nombre de dominio. El WHOIS acotado es información mínima que va a ser pública o que va a ser publicada. Esa es la diferencia básica entonces. Muchísimas gracias, Chuck.

CHUCK GOMES: Quiero agregar un solo comentario más, Tijani. Mucha gente lo sabe pero .COM y .JOB son registros acotados y ellos solo ofrecen una cantidad mínima de datos. Hay que ir al registrador para obtener todos los datos. Espero que esto aclare también parte de las dudas.

TIJANI BEN JEMAA: Muchas gracias. Antes de pasar a las preguntas, en primer lugar vamos a ir a lo que es entonces esta encuesta final o estas preguntas.

YEŞIM NAZLAR: Gracias, Tijani. Vamos a pasar entonces a lo que tiene que ver con las preguntas del final. Veo que hay algunas preguntas. Alfredo Calderón en el chat. No sé si quieren leerlas ahora o si quieren pasarlas a después de estas preguntas que hacemos al finalizar.

TIJANI BEN JEMAA: Sí. Después. Ahora vamos a hacer este breve examen, por así llamarlo. Después vemos las preguntas.

YEŞIM NAZLAR: La primera pregunta dice: ¿Es apropiado que la organización ICANN trabaje con la comunidad para tratar de desarrollar un enfoque para cumplir con el GDPR antes de mayo de 2018? A. Sí. B. No. Por favor, marquen sus respuestas.

CHUCK GOMES: ¿Estas preguntas son para Thomas y para mí o son para los participantes en este seminario web?

TIJANI BEN JEMAA: No. Son para los participantes.

CHUCK GOMES: Sí, eso pensé, pero quería asegurarme.

YEŞIM NAZLAR: Sí, Chuck. Voy a leer la respuesta correcta y que usted también la dé.

CHUCK GOMES: Sí. Obviamente. Thomas también puede intervenir porque realmente está participando activamente, incluso lidera gran parte de este trabajo, sobre todo teniendo en cuenta la fecha límite que es el 25 de mayo de 2018. La respuesta es sí. Es apropiado y es necesario porque en la actualidad lo que son los requerimientos contractuales para los registradores y los registros los pueden llevar a tener problemas con el GDPR, sobre todo los que son partes contratadas. Es importante decir que no tenemos que considerar que esto es un desarrollo de políticas. Tiene que haber políticas de emergencia que imparta la junta directiva para abordar este problema pero hay que marcar la diferencia. Esto no es desarrollo de políticas. La GNSO tiene procesos muy marcados para estas políticas. Estos son los procesos que pueden dar lugar a cambios en los contratos con los registros y los registradores.

Sí es necesario y sí es apropiado que las partes contratadas de la comunidad de la ICANN trabajen sobre esto pero, al mismo tiempo, hay que reconocer que esto no remplaza el proceso de desarrollo de políticas que se está dando. Como tenemos un proceso que es ascendente e incluye a todas las partes interesadas, este proceso de desarrollo de políticas es lento. Es decir, el PDP no se va a dar en breve.

TIJANI BEN JEMAA: Sí. Gracias, Chuck. No solo es apropiado sino que también, desde mi punto de vista, es necesario. Siguiente pregunta.

YEŞIM NAZLAR: Sí. Vamos a pasar a la pregunta número dos. La pregunta número dos es: ¿Será necesario entonces el trabajo del grupo de trabajo de PDP del RDS de siguiente generación si la ICANN tiene éxito en sus esfuerzos actuales?

TIJANI BEN JEMAA: Yeşim, antes de continuar, querría ver si Thomas tiene algo para decir respecto de la otra pregunta.

THOMAS RICKERT: Sí. Yo querría aprovechar la oportunidad para responder también a la primera pregunta. Si bien Chuck tiene razón en decir que es necesario debatirlo con la comunidad y que no es desarrollo de políticas, creo que tenemos que ser muy claros y transparentes. Los requisitos del GDPR, así como los requisitos que provienen de otras legislaciones nacionales o regionales de protección de datos, todas deben ser respetadas. La comunidad no puede darle forma a nada en el sentido de que hay un mínimo de lo que hay que hacer por los registros y los registradores y la ICANN porque si no, puede haber sanciones. Hay que cumplir. La comunidad debe ser informada de lo que está sucediendo. Yo creo que esto lo tienen que hacer sobre todo entre los registradores, los registros y la ICANN.

También necesitamos que la comunidad intervenga y se puede hacer en paralelo porque lo que le da legitimidad a todo lo que está haciendo la ICANN, los registradores y los registros, es el modelo de múltiples interesadas. Es ese proceso y es llegar a estas políticas por consenso.

Estas políticas por consenso se aplican inmediatamente a todos los registradores y a todos los registros sin necesidad de cambiar formalmente el contrato que tienen los registradores y los registros.

Hemos tenido una solución de protección de datos durante mucho tiempo y por eso necesitamos entonces las políticas por consenso para que pueda operar toda la industria sin ningún problema. Estas políticas por consenso no pueden ir por debajo de lo que son los requisitos mínimos con los que deben cumplir. Voy a citar un ejemplo. Si la comunidad dice: "Nosotros queremos que el WHOIS esté disponible para todos, como está hoy en día", quizá puede ser lo que quiere la comunidad pero no cumple con las leyes. En primer lugar, tenemos que establecer qué es lo que tienen que hacer las partes contratadas para evitar las sanciones. Eso debe ser así sí o sí. La forma en la que nosotros hacemos las cosas o si hacemos algo más, eso sí puede tener que ver con el proceso ascendente de múltiples partes interesadas y política por consenso de la ICANN.

TIJANI BEN JEMAA: Muchísimas gracias, Thomas. Yeşim, ¿podemos seguir adelante?

YEŞIM NAZLAR: Vamos a pasar a la pregunta número dos. ¿Será necesario el trabajo del grupo de trabajo de PDP de RDS de siguiente generación si la ICANN tiene éxito en sus esfuerzos actuales para desarrollar un enfoque para cumplir con el GDPR antes de mayo de 2018? ¿La respuesta es sí o no? Por favor, respondan.

CHUCK GOMES: La respuesta es sí. Yo creo que básicamente ya expliqué los motivos. El proceso de desarrollo de políticas se debe dar si queremos cambios a largo plazo, para que se den en los acuerdos con los registros y los registradores. Cualquier política de emergencia que se pueda implementar para abordar los temas que dejó muy en claro Thomas son nada más que soluciones temporarias. En definitiva, va a haber que implementar una política con los cambios apropiados para cumplir con todos los requerimientos, tanto del GDPR como otra reglamentación que surja en otras jurisdicciones porque hay muchos gobiernos, muchas jurisdicciones del resto del mundo que están implementando esto y que se va a dar a largo plazo. Definitivamente la respuesta es sí.

YEŞIM NAZLAR: Gracias, Chuck. Vamos a pasar ahora a la pregunta número tres. ¿Cuál de las siguientes afirmaciones es verdadera? A. Puedo publicar datos personales que recopilé legalmente. B. La recopilación legal no significa que pueda publicar datos personales. Por favor, les pido que voten ahora. Quizá Thomas nos pueda dar la respuesta correcta.

THOMAS RICKERT: Sí. La respuesta B es la respuesta correcta. Como lo expliqué en mi explicación, el hecho de haber recolectado datos de manera legítima no significa que uno pueda publicar los datos en el WHOIS y en el directorio de WHOIS.

YEŞIM NAZLAR: Muchas gracias, Thomas. Ahora vamos a pasar a la última pregunta. Mi empresa tiene sede central en Australia y solo atiendo a clientes de Australia y Nueva Zelanda. ¿Se aplica a mi caso el GDPR? ¿Sí o no? Por favor, indiquen su respuesta. Me gustaría que Thomas nos indicara la respuesta.

THOMAS RICKERT: Muchas gracias. Básicamente, si uno está fuera de Europa, lo cual es verdadero para Australia, y no atiende a titulares de datos en la Unión Europea, lo cual es cierto en este caso porque la empresa atiende solo a clientes de Australia y Nueva Zelanda, en este caso no se aplicaría el GDPR. La respuesta correcta es la respuesta dos.

YEŞIM NAZLAR: Muchas gracias, Thomas. Con esto finalizamos la sesión de preguntas sobre las presentaciones. Ahora le doy la palabra a Tijani.

TIJANI BEN JEMAA: Muchas gracias, Thomas. Ahora tenemos la sesión abierta de preguntas para los presentadores. A ver, tengo un comentario. Thomas, el GDPR es una oportunidad para aplicar normas regulatorias. Cuando usted habla acerca del consentimiento, estamos hablando de prestar el consentimiento para que se recaben los datos, nuestros datos. Uno no es libre entonces de dar el consentimiento porque hay un consentimiento un tanto automático que se necesita para que las empresas lleven a cabo sus actividades.

En segundo lugar, respecto del GDPR, quienes tienen los datos tienen que deshacerse de esos datos en cuanto finaliza el objetivo para el cual tenían esos datos o almacenabas esos datos. ¿Cómo controlamos esto? ¿Cómo nos aseguramos de que esto suceda? Es muy complicado. Es difícil.

THOMAS RICKERT: Tijani, por favor, ¿puede repetir la segunda pregunta?

TIJANI BEN JEMAA: Sí. Quienes recolectan los datos, recaban los datos, tienen que destruir esos datos en cuanto finaliza la actividad para la cual tenían esos datos. ¿Cómo se controla eso? ¿Cómo cerciorarse de que esto se haga?

THOMAS RICKERT: Muchas gracias por esta pregunta. Con respecto a la primera pregunta, es cierto que cuando uno se suscribe a servicios se le suele pedir el consentimiento. Hay situaciones en las cuales por ejemplo se ofrece un servicio gratuito y básicamente uno tiene que dar datos a un operador para obtener el servicio. Si ese modelo se cambia y este servicio gratuito ya no se puede ofrecer, entonces tenemos una relación directa entre el servicio y el suministro de datos. En algunos casos puede ser correcto solicitar el consentimiento sin infringir la prohibición de consentimiento acumulado. En el caso de registros, uno está pagando por un nombre de dominio y la publicación de datos en el sistema de WHOIS no es un requisito inevitable para que sea posible registrar un dominio.

En el universo de los ccTLD, uno puede registrar un nombre de dominio sin que se divulguen los datos. No decimos que sea fácil hacer esto posible pero sí sabemos que hay un alto riesgo que implica crear un sistema que necesite consentimiento para los datos de WHOIS. Probablemente haya grupos de registratarios que brinden su consentimiento y el registro pueda tener un modelo basado en consentimiento para WHOIS. Esto, por ejemplo, puede pasar en operadores de punto .BANK, .INSURANCE o dominios similares y puedo vislumbrar casos en los que los registros de esos gTLD que necesitan tanto nivel de confianza determinen que se puedan publicar los datos porque quieren facilitar que los clientes verifiquen que están haciendo transacciones con un banco genuino o con una aseguradora que existe de verdad.

Con respecto al periodo de retención de los datos, esa es una muy buena pregunta. Hay distintos periodos de retención de datos para distintos tipos de datos. Esto se torna más complejo por ejemplo en el caso de las autoridades impositivas. Las autoridades impositivas fiscales pueden requerir extensos periodos de retención de datos. Sin embargo, para brindar un servicio, ese periodo quizá no sea tan extenso. Es muy posible que uno tenga distintos plazos para retener datos para distintos elementos de datos. ¿Cómo se controla esto? Cada empresa que tiene que cumplir el GDPR tiene que tener una lista de distintos procesos para sus actividades y los distintos mecanismos de protección de datos. Tiene que tener un repositorio de políticas para el tratamiento de distintos datos y para los distintos elementos de datos. Si las autoridades le solicitan información, usted tiene que poder presentarles a las

autoridades sus políticas y poder explicarles a las autoridades qué es lo que usted hace para que los datos sean eliminados. Con lo cual, Tijani, esto es algo complejo pero también es algo viable.

Con respecto a otros aspectos, el GDPR tiene que ver con datos de las personas que son correctos. Tenemos que ver también cuestiones de jurisdicción. Por ejemplo, en Europa podemos identificar a una persona. Por ejemplo, yo tengo un estudio jurídico que se llama Estudio de Abogados Rickert. Es una empresa corporativa, una entidad GMBH en mi país. Mis datos corporativos se transforman en datos personales, con lo cual hay cierto riesgo que implica la diferenciación entre datos corporativos y datos personales porque quizá al hacer esta clasificación no se refleje en los requisitos legales.

TIJANI BEN JEMAA: Muchas gracias. Antes de darles la palabra a otros participantes, a Olivier, ¿tenemos más preguntas? Creo que Yeşim las va a leer. Adelante, Yeşim. ¿Yeşim? Yeşim, ¿me puede oír? Entonces le doy la palabra a Olivier. Olivier, tiene la palabra. ¿Olivier? No entiendo qué sucede.

GISELLA GRUBER: Tijani, estamos conectando a Olivier por teléfono en este momento.

OLIVIER CRÉPIN-LEBLOND: Hola, hola. ¿Me oyen?

TIJANI BEN JEMAA: Ahora sí.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Tijani. No recordaba que las líneas estaban silenciadas y que había que presionar *6 y *7. No lo recordaba. Tengo dos preguntas para Thomas. En primer lugar, muchas gracias por este seminario web. Es muy importante y aliento a los participantes europeos a que se involucren porque nosotros estamos en el centro de toda esta situación. Tengo una pregunta para Thomas. Usted mencionó que faltan apenas unos meses para que el GDPR entre en vigencia. Usted mencionó la posibilidad de multas. ¿Cuánto tiempo cree usted que pasará para que este reglamento pase al nivel de legislación local y cuánto tiempo cree que será necesario para que los registros y registradores de la ICANN estén listos? Como sabemos, en la próxima reunión en Puerto Rico se va a hablar mucho sobre este tema. Tenemos que lograr un consenso pero después del consenso viene la implementación. Esa pregunta es para Thomas.

Mientras Thomas prepara su respuesta, tengo una pregunta para Chuck acerca de su presentación. Sé que algunos registros están implementando un programa piloto de RDS con datos abiertos. ¿No podemos pasar directamente a la implementación, simplemente verificar cómo funciona este programa piloto del RDS en paralelo con WHOIS y así facilitar la implementación de esta nueva medida?

THOMAS RICKERT: Muchas gracias, Olivier, por su pregunta. Quizá usted no escuchó bien lo que yo dije acerca del GDPR y la legislación nacional. Tenemos el riesgo de sanciones a partir del 25 de mayo. Si bien hay otras empresas que están recabando datos personales a gran escala, corren el riesgo de que las autoridades encargadas de protección de datos quieran verificar esta situación. Hay grupos de usuarios que están esperando impugnar a registros y registradores y recurrir a las autoridades de supervisión en caso de que no se cumpla con esta norma. No tenemos más tiempo. No tenemos tiempo adicional. Incluso si los registros y registradores de la ICANN optan por un modelo en la mañana, será demasiado tarde para muchos registros y registradores para que puedan implementar los cambios técnicos. Esto requiere mucho tiempo. Algunos ya empezaron a implementar soluciones sin siquiera saber qué sucedería en la ICANN. ¿Qué pasa si se enteran de los requisitos de la ICANN solo en Puerto Rico o más adelante? No van a tener tiempo de implementar los aspectos técnicos.

También quiero aprovechar para responder a varios comentarios que se hicieron en la sala de chat acerca del GDPR en contraposición a otras leyes de protección de datos. El GDPR será aplicable solo a titulares de datos en Europa. Eso es cierto pero creo que fue GoDaddy la empresa que hizo cierta investigación acerca de otras leyes en materia de protección de datos en aproximadamente seis jurisdicciones y la respuesta es que si uno cumple con el GDPR, cumple con las leyes prácticamente en todas las jurisdicciones. Sería posible que los operadores hagan algo específico para quienes están gobernados o regidos por el GDPR pero si tenemos 70-80 regímenes de protección de

datos distintos en todo el mundo, bueno, si queremos que los registros y registradores tengan una solución para todos estos mercados, creo que desde un punto de vista operativo sería muy sensato tener una solución que se pueda aplicar a nivel mundial para evitar la segmentación del mercado.

TIJANI BEN JEMAA: Muchas gracias. ¿Pueden leer por favor las otras preguntas?

YEŞIM NAZLAR: Sí, claro, Tijani.

OLIVIER CRÉPIN-LEBLOND: Tenía una segunda pregunta, perdón.

CHUCK GOMES: Disculpen. Gracias por la pregunta. Parece que hay otra conversación en curso. ¿Desean que conteste a la segunda pregunta de Olivier?

OLIVIER CRÉPIN-LEBLOND: Sí, por favor. Deseo que conteste a mi segunda pregunta.

CHUCK GOMES: Muchas gracias. Creo que el programa piloto que usted mencionó, o programa Beta según lo denominan las distintas partes contratadas… Creo que necesitamos silenciar algunas líneas. Es importante entender el rol del protocolo versus el rol de la política. El rol del protocolo es un rol

de estándar técnico creado por el IETF y los registros y registradores ya tienen que utilizar ese protocolo de aquí en adelante aunque no lo utilicen en este momento. El grupo de trabajo mira con agrado el hecho de tener este programa piloto por parte de distintas partes contratadas para verificar el uso del protocolo, el protocolo RDAP.

Una de sus principales características es que permite el acceso restringido y eso forma parte de la carta orgánica del grupo de trabajo. El hecho de que se esté probando el protocolo no limita en modo alguno la necesidad de hacer una política. El uso del protocolo puede ser una política pero el protocolo en sí no lo es, con lo cual, hay que tener una política para definir por ejemplo cómo se utilizaría este acceso restringido con el protocolo RDAP. Creo que se nos está acabando el tiempo pero espero haber respondido su pregunta. Si no, podemos seguir conversando en esta llamada o por correo electrónico.

TIJANI BEN JEMAA: Gracias, Chuck. Yeşim, por favor.

YEŞIM NAZLAR: Gracias, Tijani. Hay un par de preguntas todavía que querría leer. Esto es de Alfredo Calderón porque es el primero y tiene un par de preguntas. ¿Qué pasa con dominios como alfredocalderon.com? No sé si las leo todas o las respuestas se dan de a una.

TIJANI BEN JEMAA: Una por una, por favor.

YEŞIM NAZLAR: Perfecto. Esta fue la primera pregunta entonces de Alfredo.

CHUCK GOMES: Voy a responder entonces. Thomas, si tiene algo para decir, por favor, intervenga. En primer lugar, debemos dejar en claro que no va a suceder nada a los DNS que están registrados a raíz del GDPR porque el nombre de dominio está registrado. Lo que va a cambiar para cumplir con los requisitos del UDRP obviamente es la información personal que tiene ese nombre de dominio. Eso es lo que tiene relación con el GDPR, sobre todo cuando el registratario es lo que en Europa se considera un sujeto interesado o el titular de los datos.

Dentro de la jurisdicción europea en relación con el GDPR, lo que se muestra en cuanto a los datos vinculados con ese dominio, eso cambia. Hoy WHOIS muestra todo a menos que haya algunos servidores de proxy o de representación. Lo que Thomas dejó muy en claro es que lo que viola el GDPR es esta muestra total de los datos.

TIJANI BEN JEMAA: Gracias, Chuck. También les pediría que las respuestas sean breves, por favor, porque solo tenemos 10 minutos más. Nos queda poco tiempo. Segunda pregunta, Yeşim.

YEŞIM NAZLAR: La segunda pregunta de Alfredo Calderón es: "¿Cómo afecta esto a Amazon, Facebook o [inaudible], que utilizan cookies?"

CHUCK GOMES: ¿Está esto vinculado con el GDPR? ¿Podrían leer la siguiente también?

TIJANI BEN JEMAA: También tenemos la siguiente.

YEŞIM NAZLAR: La siguiente es de Alfredo Calderón para Chuck. "¿El PDP del RDS de siguiente generación va a estar estrechamente vinculado con el GDPR?"

CHUCK GOMES: No.

YEŞIM NAZLAR: Y la siguiente pregunta, también de Alfredo Calderón es: "¿El trabajo de la comunidad va a mejorar los requisitos del GDPR?" Voy a continuar con las otras preguntas porque me parece que son todas pertinentes. "¿Qué va a suceder si en el futuro organizaciones o individuos de fuera de la Unión Europea trabajan en la Unión Europea?"

TIJANI BEN JEMAA: Creo que lo pueden responder Chuck o Thomas.

THOMAS RICKERT: ¿La pregunta entonces era una compañía fuera de la Unión Europea que le presta servicios a alguien dentro de la Unión Europea? En ese caso

depende de si son ciudadanos o sujetos interesados que ocasionalmente se prestan servicios. Si uno está fuera de la Unión Europea pero de vez en cuando le presta servicios a un ciudadano u organización dentro de la Unión Europea, no tiene por qué cumplir. Esa es la excepción que marca el GDPR. Ahora, si uno apunta directamente a clientes de la Unión Europea, ahí hay que cumplir plenamente con el GDPR.

TIJANI BEN JEMAA: Siguiente, por favor.

YEŞIM NAZLAR: La siguiente pregunta es de Mohamed Yusef Alhaj. "¿Cómo se pueden imponer multas en organizaciones dentro del territorio de la Unión Europea?"

THOMAS RICKERT: Me parece que es para mí también esta pregunta. Yo mencioné anteriormente que las compañías que no estaban en la Unión Europea necesitan designar un representante dentro de la Unión Europea. Esto es para la comunicación con las autoridades. Esto puede utilizarse para las sanciones pero el otro mecanismo sería acuerdos de eficiencia mutua que tienen que ver con la privacidad entre Europa y Estados Unidos, que también tienen un mecanismo implementado para que las sanciones puedan aplicarse extraterritorialmente.

TIJANI BEN JEMAA: Bien. Siguiente, por favor.

YEŞIM NAZLAR: Gracias, Thomas. La siguiente pregunta es: "¿Qué pasa con los que no son miembros de la Unión Europea como Georgia cuando existen acuerdos de asociación con la Unión Europea o entre países vecinos?"

TIJANI BEN JEMAA: Esto es para Thomas.

THOMAS RICKERT: El GDPR se va a aplicar a los estados miembros de la Unión Europea y los que están dentro de la Comunidad Económica Europea que tienen acuerdos con la Unión Europea. No estoy seguro en este momento de qué es lo que sucede exactamente con Georgia pero el principio general que mencioné es que si una compañía de Georgia le va a prestar servicios a clientes dentro de la Unión Europea y no es un cliente ocasional, entonces se va a aplicar el GDPR.

TIJANI BEN JEMAA: Gracias, Thomas. Gracias, Yeşim. Tengo dos preguntas breves para ambos. Supongo que vieron el blog con el modelo propuesto. ¿Ustedes creen que estos son los únicos modelos posibles? ¿Creen que son los pertinentes? En ese caso, ¿cuál elegirían entre el uno, el dos y el tres?

CHUCK GOMES: Thomas, me parece que esta es una pregunta que es más para usted.

THOMAS RICKERT: ¿Qué modelo elegiría? Ninguno. Yo creo que hay fallas en todos. Pido disculpas por ser tan directo pero todos los modelos que menciona la ICANN están basados en algunos principios que tienen que ver con los modelos anteriores. Uno es que los datos que se recopilan actualmente se van a recopilar con el modelo nuevo. Yo mencioné anteriormente que estoy convencido de que no se necesita lo que es admin C, técnico C, etc. Eso sería una violación de la minimización de los datos, la recopilación minimizada de los datos. Este principio, este prerrequisito que está en todos estos modelos hace que todos estos modelos tengan fallas porque los modelos solo miran la parte de divulgación pero no la parte de recopilación que tiene que ver con el procesamiento de los datos.

Esos modelos también asumen que todos los datos pueden pasarse de los registradores a los registros. Yo creo también que es una hipótesis incorrecta. Lo mencioné en mi presentación. Es posible que los datos se transfieran de un registrador a un registro pero existen otros requisitos legales que hay que cumplir para poder cumplir plenamente. Me parece que no soy el único en realidad que tiene esta visión sobre las propuestas realizadas por la ICANN.

La Comisión Europea organizó una reunión sobre Internet y tanto los comisarios como Jean Jacques Sahel, que es el representante de la comunidad dijeron: “¿Por qué se propusieron estos modelos?” Porque ellos creen que los modelos están en contra incluso del asesoramiento legal que pidió la organización.

CHUCK GOMES: Para responder a otra parte de la pregunta, Tijani, si hay otros modelos, sí. De hecho, ECO, con quien está Thomas, ha propuesto otro que no fue muy considerado aparentemente antes de que la ICANN desarrollara los tres modelos. Supongo que va a haber más modelos en el futuro.

YEŞIM NAZLAR: ¿Tijani? No podemos escucharlo. No sabemos si está hablando en este momento.

TIJANI BEN JEMAA: ¿Me escuchan ahora?

YEŞIM NAZLAR: Sí. Ahora sí.

TIJANI BEN JEMAA: Gracias. Gracias, Thomas y Chuck, por estas excelentes presentaciones y este debate que también fue muy interesante. Tenemos mucho más, obviamente pero ya nos pasamos 17 minutos del horario pautado. Tenemos entonces una parte que tiene que ver con la evaluación de este seminario web. Yeşim, por favor. Adelante con las preguntas.

YEŞIM NAZLAR: La primera pregunta de evaluación es qué le pareció el horario del seminario web. A. Demasiado temprano. B. Bien. C. Demasiado tarde. Por favor, voten. Voy a pasar ahora a la pregunta número dos. La número dos es: ¿Qué le pareció la tecnología utilizada para el seminario

web? Muy buena. Buena. Suficiente. Mala. Muy mala. Por favor, voten ahora. Vamos a pasar a la pregunta número tres: ¿Los presentadores demostraron dominio del tema? Muy fuerte. Fuerte. Suficiente. Débil. Extremadamente débil. Por favor, voten ahora. Vamos a pasar a la pregunta número cuatro. ¿Está satisfecho con el seminario web? Extremadamente satisfecho. Satisfecho. Moderadamente satisfecho. Ligeramente satisfecho. No satisfecho. Por favor, voten.

Vamos a pasar ahora a la pregunta número cinco. ¿En qué región vive en la actualidad? África. Asia, Australia y las islas del Pacífico. Europa. América Latina y el Caribe. América del Norte. Por favor, voten. Vamos a pasar a la pregunta número seis. ¿Cuántos años de experiencia tiene en la comunidad de la ICANN? Menos de uno. Entre uno y tres. Tres a cinco. 5 a 10. Más de 10 años. Finalmente, la última pregunta: ¿Qué temas le gustaría que fueran cubiertos en los futuros seminarios web? Les pedimos por favor que utilicen este espacio para escribir los comentarios. Voy a dejar esta pregunta abierta para que puedan escribir todo, quienes quieran. Después presionan el botón del costado para que nos pueda llegar.

TIJANI BEN JEMAA: Podemos poner aquí todos los otros temas porque en realidad nos interesa saber qué les interesa a ustedes. También hay un webinar sobre GDPR. Les animo a que lo sigan. Ya nos hemos pasado 21 minutos. Les quiero agradecer a todos. Les quiero agradecer a Chuck y Thomas, al personal, a los intérpretes. Gracias a todos los participantes por asistir a este seminario web. Con esto doy por finalizado este seminario.

YEŞIM NAZLAR: Con esto terminamos el seminario. Les pedimos por favor que desconecten sus líneas. Les deseo a todos una buena continuación del día. Adiós.

[FIN DE LA TRANSCRIPCIÓN]