الهيئة العامة للرقابة المالية

قرار رقم ٧٢٩ لسنة ٢٠١٦

بتاريخ ٢٠١٦/٨/٢٨

بشأن الضوابط التكنولوجية وقواعد تأمين المعلومات المرتبطة بإصدار وتوزيع شركات التأمين لبعض وثائق التأمين النمطية الكترونياً من خلال شبكات نظم المعلومات

رئيس الهيئة العامة للرقابة المالية

بعد الاطلاع على القانون رقم ١٠ لسنة ١٩٨١ بإصدار قانون الإشراف والرقابة على التأمين فى مصر ولائحته التنفيذية وتعديلاتها ؛

وعلى القانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الالكترونى فى مصر ؛

وعلى القانون رقم ١٠ لسنة ٢٠٠٩ بتنظيم الرقابة على الأسواق والأدوات المالية غير المصرفية ؛

وعلى النظام الأساسى للهيئة العامة للرقابة المالية الصادر بقرار رئيس الجمهورية رقم ١٩٢ لسنة ٢٠٠٩ ؛

وعلى مذكرة السيد المستشار نائب رئيس مجلس الدولة المستشار القانونى للهيئة بتاريخ ٢٠١٥/٩/١ ؛

وعلى قرار مجلس إدارة الهيئة رقم ١٢٢ لسنة ٢٠١٥ بشأن تنظيم إصدار وتوزيع شركات التأمين لبعض وثائق التأمين النمطية الكترونيًا من خلال شبكات نظم المعلومات ؛

قـــــرر :

(المـادة الأولى)

على شركات التأمين الحاصلة على موافقة الهيئة على إصدار وثائق تأمين نمطية الكترونيًا من خلال نظم معلومات الشركة وإتاحة طباعة الوثيقة وتوزيعها بواسطة المؤمن له مباشرة أو بواسطة إحدى الجهات التى وافقت عليها الهيئة وذلك كله وفقًا للقرار رقم ١٢٢ لسنة ٢٠١٥ أن تلتزم بالضوابط التكنولوجية وقواعد تأمين المعلومات المرفقة بهذا القرار .

(المـادة الثانية)

يُنشـر هذا القـرار بالوقـائـع المصريـة وعلى الموقـع الإلكترونـى للهيـئـة ، ويُعمل به من اليوم التالى لتاريخ نشره ، ويُبلغ إلى الإدارات المعنية لتنفيذه .

رئيس الهيئة

شريف سامى

الضوابط التكنولوجية وقواعد تأمين المعلومات المرتبطة بإصدار وتوزيع شركات التأمين لبعض وثائق التأمين النمطية الكترونياً من خلال شبكات نظم المعلومات

أولاً - البنية التحتية التكنولوجية :

يكون مركز معلومات شركة التأمين داخل حدود جمهورية مصر العربية وخاضع لقوانينها ويجوز اللجوء للتعاقد على خدمات الاستضافة (Hosting) للبنية التكنولوجية للشركة لدى جهة أخرى داخل مصر من ضمن الجهات المعتمدة من الهيئة لتقديم تلك الخدمات وفقًا لقرار رئيس الهيئة رقم ٣١٦ لسنة ٢٠١٤ ، أو لدى المساهم الرئيسى للشركة خارج مصر فى حال كونه شركة تأمين أو إحدى شركاتها التابعة أو لدى شركات أخرى متخصصة ولها سابقة أعمال فى المجال وذلك بشرط أن توافق عليها الهيئة ، يجب أن تكون شركة الاستضافة مقدمة الخدمة معتمدة من الهيئة .

١ - وسائل الاتصال :

يجب أن تكون كل وسائل الاتصال المستخدمة مصرح لها من الجهاز القومى لتنظيم الاتصالات .

٢ - الخوادم المركزية ونظم التشغيل :

تلتزم شركة التأمين باستخدام أجهزة الخوادم المركزية يتوافر فيها ما يلى كحد أدنى :

(أ) جهاز خادم مستقل يعمل كخادم لقواعد البيانات Database Server (سواء خادم مادى Physical أو باستخدام بيئة افتراضية Virtual) .

(ب) جهاز خادم مستقل يعمل كخادم للتطبيقات Application Server (سواء خادم مادى Physical أو باستخدام بيئة افتراضية Virtual) .

(جـ) أن تحقق مواصفات تلك الخوادم الحد الأدنى من متطلبات التشغيل (Hardware and Software Requirements) اللازمة لتشغيل خدمات الإصدار والتوزيع الالكترونى لوثائق التأمين وتخزين بياناتها .

(د) أن تكون جميع نظم التشغيل والبرامج الإلكترونية المستخدمة فى هذه الخوادم مرخصة ومحدثة .

(هـ) أن يتوافر بها الحد الأدنى من المستوى المطلوب من العمل الدائم دون توقف (High Availability) بمعدل لا يقل عن (٩٥٪) .

فى حال رغبة الشركة استخدام بيئة افتراضية Virtual يجب أن يتوفر بها نظام أمن معلومات يسمح بالفصل بين الخوادم باستخدام سياسات وقواعد أمن المعلومات (Security policies and rules) .

٣ - حماية وأمن المعلومات :

تلتزم الشركة بتوفير البنية التكنولوجية اللازمة لأمن المعلومات لديها (أو لدى جهة الاستضافة) وفقًا للضوابط التالية :

(أ) تركيب نظام جدار نارى Firewall لتأمين شبكات الاتصال داخل الشركة وبين الشركة والجهات الأخرى القائمة بتوزيع الوثائق ويجوز أن يكون ذلك من خلال مخارج متعددة لنفس الـ Firewall .

(ب) توفير نظم حماية للشبكة وفقًا للخدمات المطلوب حمايتها (على سبيل المثال نظام للحماية من الاختراق Intrusion Prevention System IPS) .

(جـ) إجراء الصيانة الدورية لأجهزة تأمين الشبكات والمعلومات مع مراعاة قواعد الضبط المناسبة لها (Configuration Roles) وتحديثها بصفة مستمرة .

(د) تزويد جميع أجهزة الحاسب المتصلة بشبكة الشركة (شخصية أو محمولة أو خوادم) ببرامج لمكافحة الفيروسات والبرمجيات الضارة (Antivirus and Antimalware) على أن يتم تحديثها بصفة مستمرة .

(هـ) وضع نظام للمراقبة والتحكم فى الدخول والخروج لغرفة الخوادم المركزية (Data Center) من الداخل والخارج .

(و) إبلاغ الهيئة عند حدوث أى اختراقات أمنية (Security Incident) تحدث على مستوى البنية الأساسية للمعلومات والأنظمة العاملة عليها والإجراءات المتخذة بشأنها .

(ز) فى حالة استخدام موقع إلكترونى على شبكة المعلومات الدولية لاستصدار وطباعة وثائق التأمين يجب أن يتم تأمين هذا الموقع باستخدام شهادة تأمين إلكترونية SSL (Website Digital Certificate) .

(ح) فى حال رغبة شركة التأمين فى تطبيق نظام التوقيع الإلكترونى (Digital Signature) يجب أن يكون متوافقًا مع شروط ومتطلبات هيئة تنمية صناعة تكنولوجيا المعلومات ، وليكون للتراسل بالبريد الإلكترونى مع العملاء حجية قانونية ، فإنه يجب على الشركة توثيق البريد الإلكترونى ومرفقاته باستخدام شهادة توقيع إلكترونى .

ثانيًا - المواصفات الفنية لنظام المعلومات (التطبيقات) :

١ - نظام المعلومات :

تلتزم شركة التأمين بتوفير نظام معلومات كامل ومؤمن لتسجيل ومعالجة بيانات العملاء سواء بالتعامل المباشر مع العميل أو من خلال الجهة الموزعة للوثيقة ، ويتكون النظام من التطبيقات وقواعد البيانات الخاصة بجميع التعاملات على منتجات التأمين النمطية المنصوص عليها فى القرار رقم ١٢١ لسنة ٢٠١٥

وفى جميع الأحوال يجب أن تلتزم شركة التأمين بما يلى :

(أ) عدم الاحتفاظ ببيانات العميل لدى الجهة الموزعة للوثيقة (تسجيل البيانات والاحتفاظ بها على قاعدة البيانات تكون لدى شركة التأمين فقط) .

(ب) الحفظ الإلكترونى لدى الشركة لكامل بيانات الوثيقة وشروطها (لتجنب حالات الاقتصار على بيانات العميل وباقى بيانات جدول الوثيقة والإشارة إلى شروط نمطية Template يمكن تعديلها لاحقًا) .

(جـ) أن تكون بيانات الوثيقة التى تظهر على الشاشة والنسخ المطبوعة متفقة مع البيانات التى حددتها الهيئة .

(د) يجب أن يحتوى النظام على علامة مميزة أو رمز للخانات الإجبارية مرتبطة برسائل تنبيهية تظهر للمستخدم حالة إدخال بيانات غير متوافقة مع طبيعة بيانات الخانة .

(هـ) يجب أن يصدر النظام رقمًا موحداً (Unique number) لكل وثيقة ، على أن يكون مسلسلاً وغير متكرر ، وذلك بخلاف رقم الوثيقة (Policy Number) .

(و) الوثيقة لا تصدر ولا يتم إصدار رقم لها إلا بعد التأكد من إدخال جميع البيانات وإظهار للعميل صفحة قابلة للطباعة للمراجعة ويكون بها جميع البيانات المدخلة وجميع شروط الوثيقة ، ويكون للمستخدم بعد ذلك خيار تأكيد قبوله لإصدار الوثيقة أو رفضه من خلال الصلاحيات الممنوحة للمستخدم .

(ز) على النظام أن يمنع تعديل أو مسح أى بيانات أو معلومات بعد إصدار الوثيقة ، ويمكن إلغاء الوثيقة دون حذفها من النظام وتبقى بما يشير إلى أنها ملغاة على قاعدة بيانات الشركة بنفس رقم الوثيقة .

(ح) أن يتيح النظام للعميل إمكانية الاطلاع وطباعة شروط الوثيقة فى أى مرحلة من مراحل التسجيل أو المراجعة أو بعد صدور الوثيقة .

٢ - تأمين دخول المستخدم :

(أ) يجب أن يمنع النظام دخول نفس اسم المستخدم أكثر من مرة واحدة فى نفس الوقت أو فتح أكثر من اتصال Session بواسطة نفس اسم المستخدم فى نفس الوقت .

(ب) يجب ألا يسمح النظام باستمرار الاتصال غير الفعال مع العميل مباشرة أو الجهة الموزعة للوثيقة (Inactive Session) لأكثر من ٢٠ دقيقة ويطلب بعدها النظام إعادة إدخال بيانات التحقق مرة أخرى .

(جـ) يجب أن يسمح النظام للعميل أو الجهة الموزعة للوثيقة بتغيير كلمة السر بنفسه فى أى وقت ، كما يجب أن يجبر النظام المستخدم (الجهة الموزعة للوثيقة أو المستفيد) على تغيير كلمة السر عند أول استخدام فى حالة صدور أو تغيير كلمة السر من قِبَل شركة التأمين نفسها ، على أن تتبع القواعد المعمول بها فى إنشاء كلمة السر بحيث يصعب استنتاجها أو التعرف عليها (لا تقل عن ٨ حروف وأرقام ، يجب أن تحتوى على رموز ولا تكون سهلة الاستنتاج والتخمين) .

(د) فى حالة تعامل العميل مع الشركة مباشرة يمكن للعميل تسجيل حساب جديد على الموقع الالكترونى للشركة ، على أن يتم التحقق من العميل عن طريق إرسال بريد الكترونى للتحقق من هويته أو إرسال رسالة نصية إلى رقم هاتف محمول يحدده العميل .

(هـ) فى غير حالات التعامل المباشر بين العميل والشركة ، أى وجود جهة قائمة بتوزيع الوثائق - فى الحالات التى سمح بها القرار رقم ١٢٢ لسنة ٢٠١٥ - لا يمكن للعاملين بالجهة تسجيل أنفسهم على نظام شركة التأمين أو موقعها الإلكترونى مباشرة ولكن يتم فتح حساب إلكترونى لهم من خلال الشركة ، وتكون الشركة مسئولة عن تأمين كلمة السر التى تمنحها لأىٍ منهم .

(و) فى حالة وجود أكثر من مستخدم لدى الجهة القائمة بالتوزيع يجب على شركة التأمين إنشاء حساب لكل مستخدم على حدة ، كما يجب على الوسيط إخطار شركة التأمين عند أى تغيير يطرأ على المستخدمين لنظام الشركة .

(ز) يجب أن يجبر النظام كافة المستخدمين على تغيير كلمة السر كل ٩٠ يومًا على الأكثر .

(ح) يجب على نظام الشركة تسجيل العنوان الإلكترونى للمستخدم وقت الدخول IP Address .

ثالثاً - ضوابط عامة :

١ - ضبط التوقيت :

تلتزم شركة التأمين بضبط توقيتات (Time Synchronization) لجميع أنظمة المعلومات والأجهزة المثبت عليها هذه الأنظمة وجميع أنظمة الشبكات وأمن المعلومات على توقيت واحد يكون مماثلاً لتوقيت جمهورية مصر العربية .

٢ - التسجيل والحفظ بالسجلات :

تلتزم شركة التأمين بما يلى :

(أ) تسجيل جميع الأنشطة Logging Activities التى تحدث على جميع الأجهزة والأنظمة (System Logs, Security Logs and Application Logs) وما تعتمد عليه من أجهزة مساعدة (حاسبات ، أجهزة شبكات ، أجهزة تأمين معلومات) .

(ب) تسجيل جميع محاولات الدخول والخروج من النظام لكل من العميل / الجهة الموزعة للوثيقة / موظفى الشركة - (الناجحة أو الفاشلة منها) وأن يشمل التسجيل الرقم المميز Unique Session ID .

(جـ) تسجيل بيانات المستخدم القائم بإدخال البيانات :

١ - فى حالة التعامل المباشر مع العميل يقوم النظام بتسجيل اسم المستخدم القائم بإدخال البيانات .

٢ - فى حالة التعامل مع جهة موزعة للوثيقة يجب أن يقوم النظام بتسجيل اسم الجهة واسم المستخدم القائم بالإدخال ، وعلى أن تكون تلك البيانات غير قابلة للتعديل (Tamper Proof) .

(د) يجب أن يقوم النظام بحفظ سجلات مستقلة للعمليات التالية :

١ - الدخول والخروج من النظام (Login ، Logoff) .

٢ - النموذج الإلكترونى لطلب إصدار الوثيقة (Form Submission) .

ويجب أن يتم الاحتفاظ بجميع السجلات (Logs) المشار إليها فى هذا القرار لمدة لا تقل عن خمس سنوات ، وفى حالة وجود نزاع مع أحد العملاء تلتزم الشركة بالاحتفاظ بكافة السجلات لحين تسوية النزاع أو صدور حكم قضائى نهائى فيه .

٣ - النسخ الاحتياطية (Backup) :

تلتزم شركة التأمين بحفظ نسخ احتياطية لكافة البيانات المشار إليها فى هذا القرار بحيث تضمن استعادة تلك البيانات حال الرجوع إليها عند الحاجة .

ويتم حفظ نسخ إضافية من النسخ المشار إليها أعلاه فى موقع بديل ، مع مراعاة أن يتم تبنى وتطبيق سياسة مكتوبة وواضحة لتسلسل النسخ ومدة الاحتفاظ .

٤ - الخصوصية :

يقتصر استخدام بيانات العميل للغرض الذى أدخلت من أجله ، وحماية خصوصية العميل وعدم إتاحة بياناته الشخصية لأى أغراض تسويقية بالاتصال الهاتفى أو الإلكترونى من قِبَل الجهة الموزعة للوثيقة أو المصدرة لها ، وعدم إتاحة تلك البيانات لأى طرف آخر .