

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

مشروع اللائحة التنفيذية لقانون المعاملات الإلكترونية

إعداد

اللجنة المشكلة بموجب قرار السيد/ مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

رقم 6 لسنة 2025م

المحتويات

الفصل الأول..... 10

الأحكام العامة..... 10

المادة (1): تعريفات..... 10

المادة (2): أهداف اللائحة..... 15

المادة (3): مجال سريان اللائحة..... 15

المادة (4)..... 15

المادة (5): حالات مستثناة من الخضوع للائحة..... 16

المادة (6): التزام الحكومة بتشجيع العمل بالوسائل الإلكترونية..... 16

المادة (7): قبول الحكومة للتعامل الإلكتروني..... 16

الفصل الثاني..... 16

التوقيع الإلكتروني والمحررات الإلكترونية..... 16

المادة (8): ضوابط إنشاء التوقيع الإلكتروني..... 16

المادة (9): صور التوقيع الإلكتروني..... 17

المادة (10): شروط صحة التوقيع الإلكتروني..... 17

المادة (11): التزامات صاحب التوقيع الإلكتروني..... 17

المادة (12): مسؤولية صاحب التوقيع الإلكتروني..... 18

المادة (13): التثبت صحة التوقيع الإلكتروني..... 18

المادة (14): التوقيع الإلكتروني المنشأ في الخارج..... 18

المادة (15): شروط استيفاء شرط الكتابة الإلكترونية..... 18

المادة (16): ضوابط حفظ المحررات الإلكترونية..... 18

المادة (17): شروط الوثيقة الإلكترونية الأصلية..... 19

المادة (18): حجية النسخة الورقية والدعامة الإلكترونية..... 19

المادة (19): شروط حجية السجلات والرسائل الإلكترونية..... 19

المادة (20): شروط نسبة الرسالة الإلكترونية إلى المنشئ..... 19

المادة (21): نسبة الرسالة الإلكترونية إلى المرسل إليه..... 20

المادة (22): الإقرار بتسلم الرسالة الإلكترونية..... 20

المادة (23): تحديد وقت بعث الرسالة الإلكترونية..... 20

المادة (24): تحديد وقت تسلم الرسالة الإلكترونية..... 20

المادة (25): تحديد مكان إرسال الرسالة الإلكترونية وتسلمها 20
المادة (26): 21
المادة (27): تعدد التوقيعات الإلكترونية على ذات المحرر 21
المادة (28): أثر تعديل المحرر الإلكتروني بعد التوقيع 21
المادة (29): توقيع الأطراف ذوي الإعاقة أو المساعدة التقنية 21
المادة (30): اللغة والمحتوى في التوقيع الإلكتروني 21
المادة (31): استخدام التوقيع الإلكتروني في العقود الرسمية 22
المادة (32): ختم الزمن الإلكتروني 22
المادة (33): حجية ختم الزمن الإلكتروني 22
المادة (34): التزامات مزودي خدمة ختم الزمن الإلكتروني 22
المادة (35): حجية ختم الزمن الإلكتروني الصادر في الخارج 22
المادة (36): ختم الزمن الإلكتروني للجهات العامة 22
المادة (37): المعايير التقنية لختم الزمن الإلكتروني 23
المادة (38): بيانات السجل الإلكتروني 23
المادة (39): ضوابط وآليات استرجاع السجلات والمستندات الإلكترونية 23
المادة (40): المعني بحفظ السجلات الإلكترونية 23
المادة (41): المدة الزمنية لحفظ السجلات الإلكترونية. 24
المادة (42): شروط حفظ السجلات الإلكترونية 24
المادة (43): حفظ المستندات والرسائل الإلكترونية 24
المادة (44): حجية الصور المنسوخة 24
المادة (45): تحقق المحكمة من صحة السجل أو الرسالة 24
المادة (46): حجية المحرر الإلكتروني 25
المادة (47): الآثار القانونية المترتبة على المعاملات الإلكترونية 25
الفصل الثالث 25
التصديق الإلكتروني 25
المادة (48): 25
المادة (49): منح رخص المزاولة لمقدمي خدمات التصديق 25
المادة (50): التحقق من التزام مقدم خدمات التصديق 26

المادة (51): إصدار وتسليم وحفظ شهادات المصادقة الإلكترونية..... 26
المادة (52): ضوابط إصدار شهادة المصادقة الإلكترونية..... 26
المادة (53): بيانات شهادات المصادقة الإلكترونية..... 26
المادة (54): ضوابط تسليم الشهادة..... 27
المادة (55): ضوابط حفظ الشهادات وسجلاتها..... 27
المادة (56): ضوابط حفظ وتخزين السجلات..... 27
المادة (57): ضوابط قائمة الشهادات الملغاة والمعلقة..... 28
المادة (58): ضوابط التصحيح والإلغاء..... 28
المادة (59): استيراد أو الترخيص باستيراد أدوات التشفير..... 28
المادة (60): المعايير الأمنية..... 29
المادة (61): منح الرخص للمواقع الإلكترونية ومراقبتها..... 29
المادة (62): شروط مزاولة نشاط مقدم خدمات التصديق الإلكتروني..... 29
المادة (63): الشروط المرعية في طالب الترخيص..... 29
المادة (64): إصدار وتسليم وحفظ الشهادات..... 30
المادة (65): محتويات كراس الشروط..... 30
المادة (66): وسائل موثوق بها لإصدار وحفظ الشهادات..... 30
المادة (67): السجل الإلكتروني لشهادات المصادقة..... 31
المادة (68):..... 31
المادة (69): جمع المعلومات لإصدار الشهادة..... 31
المادة (70): بيانات شهادة المصادقة..... 32
المادة (71): التزام مقدم الخدمة بضمان صحة البيانات..... 32
المادة (72): التدقيق في هوية ممثل الشخص الاعتباري..... 32
المادة (73): ضوابط تعليق وإلغاء الشهادات..... 33
المادة (74): إلغاء شهادة التصديق..... 33
المادة (75): حالات إلغاء الشهادة..... 33
المادة (76): التزامات ومسؤوليات صاحب الشهادة..... 34
المادة (77): التزامات مقدم خدمات التصديق الإلكتروني..... 34
المادة (78): مسؤوليات مقدم خدمات التصديق الإلكتروني..... 35

المادة (79) : الاعتراف بالشهادات الأجنبية.....35
المادة (80): إيقاف نشاط مقدم خدمات التصديق الإلكتروني.....35
المادة (81): تحويل نشاط مقدم خدمات التصديق الإلكتروني.....35
الفصل الرابع.....36
المعاملات الإلكترونية.....36
المادة (82): التعبير عن نية التعاقد الإلكتروني.....36
المادة (83):.....36
التزامات البائع.....36
المادة (84): الالتزام بالإعلام.....36
المادة (85):.....37
المادة (86): التزامات البائع في البيع بالتجربة.....37
المادة (87):التزامات البائع عند الاخلال بالعقد.....37
التزامات البائع عند إلغاء العقد.....37
المادة (88): توفير أيقونة خاصة بالإلغاء.....37
المادة (89): حالات خاصة من الإلغاء.....38
المادة (90): الإخطار بالإلغاء.....38
المادة (91): حالات لا يجوز فيها للمستهلك إلغاء العقد.....38
مادة (92): الغاء العقد المرتبط بقرض.....38
المادة (93): فسخ العقد بسبب إخلال البائع بالتزاماته.....39
زمان ومكان العقد.....39
المادة (94): زمان الإبرام ومكانه.....39
المادة (95): زمان التنفيذ ومكانه.....39
المادة (96): عبء الإثبات.....39
المادة (97): القانون الواجب التطبيق على العقد.....39
الفصل الخامس.....40
حماية المعاملات الإلكترونية.....40
المادة (98):.....40
مادة (99): طرق حماية نظم المعلومات.....40

المادة (100): طلب فحص المعلومات..... 40
المادة (101): نظام التطبيق والالتزام..... 40
المادة (102): الحوكمة والمسؤوليات..... 41
المادة (103): المراقبة والقدرات التشغيلية..... 41
المادة (104): استطلاع التهديدات..... 41
المادة (105): الاستجابة للحوادث الأمنية..... 41
المادة (106): الضوابط الوقائية والتقنية..... 42
المادة (107): مراقبة الطرفيات والأطراف الثالثة وسلسة التوريد..... 42
المادة (108): الاختبارات والتأكد المستقل..... 42
المادة (109): مؤشرات الأداء والمخاطر والتقارير..... 43
الفصل السادس..... 43
(العمليات المصرفية)..... 43
المادة (110): الالتزام بالمعايير الملائمة للأمن السيبراني..... 43
المادة (111): العقود المنظمة للعلاقة مع العملاء..... 43
المادة (112): الشفافية والعلانية..... 44
المادة (113): آليات الاعتراض والتظلم وتسوية النزاعات..... 44
المادة (114): حماية البيانات والخصوصية..... 44
المادة (115): إصدار واستعمال البطاقات المصرفية..... 44
المادة (116): الإلغاء والتعديل والرجوع في أوامر الدفع..... 45
المادة (117): النقود الإلكترونية وإصدارها..... 45
المادة (118): التوعية..... 45
المادة (119): المسؤولية في حالة الهجمات السيبرانية..... 45
المادة (120): الالتزام المؤسسي بالدفع الإلكتروني..... 45
المادة (121): الصكوك الإلكترونية..... 46
المادة (122): السفتجة الإلكترونية..... 46
مادة (123): السند الإذني الإلكتروني..... 46
الفصل السابع..... 47
حماية البيانات الخاصة..... 47

جمع البيانات 47
المادة (124): أهداف نظام حماية البيانات 47
المادة (125): ضوابط جمع البيانات 47
المادة (126): الموافقة على جمع البيانات ومعالجتها 47
المادة (127): توثيق الموافقة وسحبها 48
المادة (128): جمع البيانات دون موافقة 48
المادة (129): شروط جمع البيانات ومعالجتها والاحتفاظ بها 48
المادة (130): حق النفاذ إلى البيانات 48
المادة (131): آلية تقنية للنفاذ إلى البيانات 49
المادة (132): ضمان سرية البيانات 49
المادة (133): نموذج جمع البيانات 49
المادة (134): طرق جمع البيانات 49
معالجة البيانات: 50
المادة (135): ضوابط معالجة البيانات 50
المادة (136): التزام مقدمي الخدمات بالإخطار 50
المادة (137): الالتزام بضوابط الخصوصية الإدارية 50
تخزين البيانات 51
المادة (138): حفظ البيانات 51
المادة (139): تحويل البيانات للخارج 51
المادة (140): تشفير البيانات 51
إدارة حوادث البيانات 51
المادة (141): اعتماد سياسة وخطة لإدارة حوادث البيانات 51
المادة (142): الإبلاغ عن حوادث البيانات 51
حذف وإتلاف البيانات 52
المادة (143): طلب حذف أو إتلاف البيانات 52
المادة (144): قيود على إتلاف البيانات 52
المادة (145): قيود إضافية عامة 52
الفصل الثامن 52

الجزاءات والمخالفات 52
المادة (146): مخالفة شروط صحة التوقيع الإلكتروني 52
المادة (147): الإخلال بحماية بيانات إنشاء التوقيع 53
المادة (148): تعديل المحررات الإلكترونية بعد التوقيع 53
المادة (149): فقدان شروط الحفظ الإلكتروني 53
المادة (150): مزاولة نشاط التصديق الإلكتروني دون ترخيص 53
المادة (151): إصدار شهادات دون تحقق أو ببيانات غير صحيحة 53
المادة (152): عدم تحديث الشهادات الملغاة أو المعلقة 53
المادة (153): الاحتفاظ بعناصر إنشاء التوقيع الخاصة بالمستخدمين 54
المادة (154): الإخلال بإجراءات الإخطار في حالات التعليق أو الإلغاء 54
المادة (155): مخالفة التزامات الإفصاح في التجارة الإلكترونية 54
المادة (156): التأخر في تسليم المنتجات أو الخدمات 54
المادة (157): عدم توفير آلية إلغاء إلكترونية 54
المادة (158): مخالفة المصارف لمعايير الأمن السيبراني 54
المادة (159): فرض رسوم غير معلن عنها 54
المادة (160): فرض رسوم غير معلن عنها 55
المادة (161): عدم تمكين صاحب البيانات من حقوقه 55
المادة (162): تشغيل مواقع إلكترونية دون ترخيص 55
الفصل التاسع 55
الأحكام العامة والختامية 55
المادة (163): 55
المادة (164): 55
المادة (165): 56
المادة (166): 56
المادة (167): 56

- الإعلان الدستوري الصادر بتاريخ 13 أغسطس 2011 ميلادي وتعديلاته.
- الاتفاقيات الدولية التي صادقت عليها الدولة الليبية.
- وعلى القانون المالي للدولة.
- وعلى قانون المرافعات، وتعديلاته.
- وعلى القانون المدني، وتعديلاته.
- وعلى قانون العقوبات، وتعديلاته، والقوانين المكملة له.
- وعلى القانون رقم (76) لسنة 1972م بشأن المطبوعات.
- وعلى القانون رقم (5) لسنة 1990م بشأن النظام الوطني للمعلومات والتوثيق.
- وعلى القانون رقم (1) لسنة 2005م بشأن المصارف وتعديلاته.
- وعلى القانون رقم (12) لسنة 2010 م بإصدار قانون علاقات العمل ولائحته التنفيذية.
- وعلى القانون رقم (22) لسنة 2010م بشأن الاتصالات.
- وعلى القانون رقم (23) لسنة 2010م بشأن النشاط التجاري وتعديلاته.
- وعلى القانون رقم (5) لسنة 2022م بشأن مكافحة الجرائم الإلكترونية.
- وعلى القانون رقم (6) لسنة 2022م بشأن المعاملات الإلكترونية.
- وعلى القانون رقم (10) لسنة 2023م بشأن التحكيم التجاري الليبي.
- وعلى لائحة الميزانية والحسابات والمخازن وتعديلاتها.
- وعلى قرار مجلس الوزراء رقم (28) لسنة 2013 م بشأن إنشاء الهيئة الوطنية لأمن وسلامة المعلومات.

الفصل الأول

الأحكام العامة

المادة (1): تعريفات

في نطاق تطبيق أحكام هذه اللائحة، ومع مراعاة معاني المصطلحات الواردة بقانون المعاملات الإلكترونية، يقصد بالعبارات والألفاظ الواردة بها المعاني المقابلة لها ما لم يدل السياق على خلاف ذلك:

1. **المعاملة الالكترونية:** كل تبادل، أو اتفاق، أو تعاقد يتم بوسيلة الكترونية، ينشئ، أو يعدل، أو ينهي التزامات قانونية.
2. **الوسيلة الالكترونية:** أي أداة تعتمد تقنيات إلكترونية، أو رقمية، أو مغناطيسية، أو ضوئية تستخدم لإنشاء، أو إرسال، أو استلام، أو تخزين المعلومات.
3. **الوثيقة الإلكترونية:** بيانات تنشأ، أو ترسل، أو تستقبل، أو تخزن بوسيلة إلكترونية، ويمكن الرجوع إليها لاحقا.
4. **الكتابة الإلكترونية:** كل حروف، أو أرقام، أو رموز، أو أي علامات أخرى تُثبت على دعامة إلكترونية، أو رقمية، أو ضوئية، أو أية وسيلة أخرى مشابهة، وتعطي دلالة قابلة للإدراك.
5. **المحرر الإلكتروني:** رسالة بيانات تتضمن معلومات تُنشأ أو تدمج، أو تخزن، أو ترسل، أو تستقبل كلياً، أو جزئياً بوسيلة إلكترونية، أو رقمية، أو ضوئية، أو بأية وسيلة أخرى مشابهة.
6. **وسيط التوقيع الإلكتروني:** أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني.
7. **السند الإلكتروني:** هو القيد، أو العقد، أو المراسلة، التي تُنشأ، أو ترسل، أو تسجل، أو تسلم، أو تحفظ، بوسيلة إلكترونية، أو على وسيط إلكتروني، ويمكن استخراجها بشكل مفهوم.
8. **الموقّع:** الشخص الطبيعي أو المعنوي الذي يستخدم توقيعا الكترونيا معتمداً.
9. **الهيئة:** الهيئة الوطنية لأمن وسلامة المعلومات.
10. **الخدمة الالكترونية:** إي خدمة تقدم، أو تنجز باستخدام الوسائط الإلكترونية، بما في ذلك الخدمات الحكومية، والخدمات التجارية.
11. **النظام الالكتروني:** مجموعة من البرمجيات والأجهزة التي تستخدم لإنشاء، أو ارسال، أو استقبال، أو معالجة، أو تخزين المعلومات الإلكترونية.
12. **بيانات إنشاء التوقيع الإلكتروني:** عناصر متفردة خاصة بالمُوقع وتميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، التي تُستخدم في إنشاء التوقيع الإلكتروني.
13. **الختم الإلكتروني:** هو توقيع إلكتروني يسمح بتحديد الشخص المعنوي مُنشئ الختم ويميزه عن غيره.

14. **منشئ الختم:** الشخص الاعتباري الحائز على بيانات إنشاء الختم الإلكتروني واستخدامه.
15. **بيانات إنشاء الختم الإلكتروني:** عناصر متفردة خاصة بمُنشئ الختم الإلكتروني، وتميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، والتي تُستخدم في إنشاء الختم الإلكتروني.
16. **شهادة الختم الإلكتروني:** الشهادة التي تصدر من الجهة المرخص لها بالتصديق، وتثبت الارتباط بين منشئ الختم وبيانات إنشاء الختم الإلكتروني.
17. **البصمة الزمنية الإلكترونية:** ما يوضع على محرر إلكتروني، ويتخذ شكل حروف، أو أرقام، أو رموز، أو إشارات، أو غيرها من بيانات ترتبط بوقت محدد لإثبات وجود هذا المحرر الإلكتروني في ذلك الوقت.
18. **تقنية شفرة المفتاحين العام والخاص:** منظومة تسمح لكل شخص طبيعي أو معنوي بأن يكون لديه مفتاحان متفردان أحدهما عام متاح إلكترونياً، والآخر خاص يحتفظ به الشخص على درجة عالية من السرية.
19. **المفتاح العام:** أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة، وتستخدم في التحقق من شخصية المُوقع على المحرر الإلكتروني، والتأكد من صحة وسلامة محتوى هذا المحرر.
20. **المفتاح الخاص:** أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة، ويتم الاحتفاظ بها على أداة إنشاء التوقيع الإلكتروني، وتُستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية.
21. **المفتاح الجذري:** أداة إلكترونية تنشأ بواسطة عملية حسابية خاصة، وتستخدمها جهات التصديق الإلكتروني؛ لإنشاء شهادات التصديق الإلكتروني، وبيانات إنشاء التوقيع الإلكتروني.
22. **خدمة ختم الزمن الإلكتروني:** هي عملية توثيق زمن إنشاء، أو إرسال، أو استلام، محرر إلكتروني، أو توقيع إلكتروني، من خلال ربطه برمز زمني مؤمَّن وصادر عن مزود خدمة مرخص له من الهيئة.
23. **الرسالة الإلكترونية** :كل رسالة بيانات تُنشأ، أو تُرسل، أو تُستقبل، أو تُحفظ، بوسيلة إلكترونية، ويُمكن إسنادها إلى منشئ محدد، والتحقق من وقت الإرسال والاستلام.
24. **المنشئ** :الشخص الطبيعي أو الاعتباري الذي تُنسب إليه الرسالة الإلكترونية ابتداءً، سواء أرسلها بنفسه، أم بواسطة نظام تابع له.
25. **المرسل** :الطرف الذي يبعث الرسالة الإلكترونية إلى المرسَل إليه عبر نظام معلومات تحت سيطرته، أو تفويضه.
26. **المرسل إليه** :الطرف الذي تُوجَّه إليه الرسالة الإلكترونية وتدخل نظام معلوماته لغرض الاستلام.

27. **نظام المعلومات** :مجموعة الموارد التقنية (أجهزة، برمجيات، شبكات، قواعد بيانات ...) المخصصة لإنشاء الرسائل الإلكترونية ومعالجتها وحفظها واستلامها.
28. **سجل الإرسال الإلكتروني** :سجل زمني معتمد، يُثبت خروج الرسالة من نطاق سيطرة المنشئ، ووقت ذلك، والإجراءات الفنية المرافقة.
29. **إشعار/إقرار الاستلام** :رسالة، أو سلوك، أو اتصال آلي، يفيد علم المرسَل إليه بوصول الرسالة الإلكترونية إلى نظامه، أو عنوانه، دون دلالة على مطابقة المضمون.
30. **مقر العمل (لأغراض الإرسال/الاستلام)** :المقر الرسمي للمرسل أو المرسل إليه المعتمد لتحديد مكان الإرسال والاستلام، ومع تعدد المقرات يُعتد بالمقر الأقرب للمعاملة، أو بالمقر الرئيسي.
31. **السجل الإلكتروني** :كل وعاء بيانات إلكتروني يُنشأ، أو يُعدَّل، أو يُحفظ، أو يُسترجع، بوسائل إلكترونية، ويُوفِّر إمكانية التتبع والتحقق من المصدر، والزمن، والمحتوى.
32. **الدعامة الإلكترونية (وسيط التخزين)** :الوسيط المادي/المنطقي، الذي تُثبت عليه البيانات، أو المحررات الإلكترونية، مع تأمين سريتها، وسلامتها، وإتاحتها للفحص.
33. **مقدّم خدمات التصديق الإلكتروني** :شخصٌ مرخّص يقدّم خدمات إصدار، وتعليق، وإلغاء الشهادات الرقمية، وخدمات التحقق ذات الصلة، وفق ضوابط الجهة المختصة.
34. **شهادة المصادقة الإلكترونية (الشهادة الرقمية)** :وثيقة إلكترونية تربط بين شخص (طبيعي / اعتباري) ومفتاح عام معيّن، تتضمن بيانات الهوية، وفترة الصلاحية، والرقم التسلسلي، وجهة الإصدار، والغرض من الاستخدام.
35. **أداة/منظومة إنشاء التوقيع الإلكتروني**: أجهزة، وبرمجيات، وإجراءات، تحت سيطرة صاحب التوقيع، تُستخدم حصراً لإنشاء توقيع إلكتروني، مع ضمان سرية المفتاح الخاص، ومنع وصول الغير إليه.
36. **الختم الزمني** :قيمة بيانات مُوقَّعة رقمياً، تربط محرراً، أو توقيعاً إلكترونياً، بلحظة زمنية محددة صادرة من مزود مرخّص، ويُمكن التحقق منها لاحقاً.
37. **مزود خدمة ختم الزمن الإلكتروني** :جهة مرخّصة تُصدر أختاماً زمنية، وفق معايير زمنية وتشفيريه معتمدة، وتحتفظ بسجلات العمليات لفترة محددة.
38. **قائمة إبطال الشهادات** :قائمة منشورة تحدّث دورياً، تتضمن الشهادات المُلغاة، أو المُعلَّقة، مع أسباب ووقت الإبطال.
39. خدمة التحقق من حالة الشهادة :خدمة تحقق فوري عبر واجهة برمجة تطبيقات؛ للتحقق من صلاحية الشهادة الرقمية، وقت الطلب.

40. **سجل الشهادة** :السجل التقني والإجرائي المرتبط بكل شهادة منذ إصدارها حتى تعليقها أو إلغائها، بما في ذلك طلبات الإصدار، والتعديلات، ووقائع التحقق والإلغاء.
41. **الشيك الإلكتروني** (الصك الإلكتروني): محرّر إلكتروني، يتضمن أمراً غير معلّق على شرط، موجهاً إلى مصرف، بدفع مبلغ معين من النقود، عند الاطلاع، ويوقَّع إلكترونياً، وفق الضوابط المعتمدة، وقابل للتداول بطريق التدوير الإلكتروني الموقّع.
42. **السفتجة الإلكترونية** :محرّر إلكتروني، مستوفٍ لبيانات السفتجة وفق القانون التجاري، قابل للتداول بطريق التدوير الإلكتروني الموقّع.
43. **السند الإذني الإلكتروني** :محرّر إلكتروني، مستوف لبيانات السند الإذني وفق القانون التجاري، قابل للتداول بطريق التدوير الالكتروني الموقّع.
44. **التدوير الإلكتروني** :انتقال الحقوق الثابتة في السفتجة/السند الإذني/الصك، إلكترونياً، عبر تظهير رقمي موقّع، يثبت تسلسل الحيازة.
45. **نظام المقاصة الإلكترونية** :منظومة تسوية وتصفية إلكترونية، لتبادل تعليمات الدائن والمدين، بين الجهات المالية حتى التسوية النهائية.
46. **كشف الحساب الإلكتروني** :بيان دوري إلكتروني بالحركات، والأرصدة، يُنشأ ويُسلَّم بوسائل إلكترونية، ويمكن التحقق من مصدره وسلامته.
47. **الدفع الإلكتروني** :كل عملية سداد تُنفَّذ بوسائل وقنوات رقمية معتمدة، تؤدي إلى انتقال قيمة مالية بين أطراف المعاملة، مع إثبات الهوية، والزمن، وسلامة العملية.
48. **التحويل الإلكتروني للأموال** :نقل قيمة مالية من حساب/محفظة إلى آخر/أخرى، عبر أنظمة معلومات، أو شبكات دفع إلكترونية، مع توثيق المُرسِل، والمُستفيد، والزمن.
49. **البيانات الشخصية (بيانات العملاء:)** كل معلومة تتعلق بشخص طبيعي مُحدّد أو قابل للتحديد، بطريقة مباشرة أو غير مباشرة، بما في ذلك مُعرِّفات الهوية، وبيانات الاتصال، والمعاملات.
50. **الشخص المعني بالبيانات** :الشخص الطبيعي الذي تتعلق به البيانات الشخصية محل الجمع أو المعالجة.
51. **حوادث البيانات** :أي واقعة أمنية تؤدي إلى إفشاء، أو تعديل، أو فقد، أو إتلاف، أو إتاحة غير مصرّح بها، للبيانات، أو الأنظمة المعالجة لها.
52. **التشفير** :تحويل البيانات إلى صيغة غير مقروءة لغير المخولين، باستخدام خوارزميات معتمدة، وإدارة مفاتيح مستقلة، أثناء النقل والتخزين.
53. **إدارة مفاتيح التشفير** :السياسات، والإجراءات، والوسائل التقنية، لإنشاء المفاتيح، وتوزيعها، وتدويرها، وتخزينها، وإبطالها، بشكل مستقل عن أماكن تخزين البيانات.

54. **المصادقة البيومترية:** التحقق اللحظي من هوية الشخص، باستخدام خصائص حيوية معتمدة، دون الاحتفاظ الدائم بالبيانات البيومترية.
55. **البوابة الإلكترونية :**موقع إلكتروني مُؤمَّن، يُنشر عبره ما تقرره الجهة المختصة من قوائم، وسجلات، وتعليمات، وخدمات تحقق عامة.
56. **واجهة برمجة التطبيقات :**واجهة تقنية تتيح الوصول الآمن لخدمات التحقق، ونشر، وتلقي طلبات المعلومات آلياً، وفق معايير معتمدة
57. **البيانات الشخصية أو بيانات العملاء:** منفردة أو مجتمعة مع غيرها — تؤدي إلى تحديد هوية شخص طبيعي بشكل مباشر أو غير مباشر، أو تجعل هذا الشخص قابلًا للتعرّف عليه، سواء كانت هذه المعلومة رقمية أو ورقية أو صوتية أو مرئية.
58. **التقابل الإلكتروني:** هو الإطار أو العلاقة القانونية والتقنية التي تربط السجل أو المحرر الإلكتروني بسياقه الكامل، بما يشمل هوية منشئه، والغرض منه، ووقت ومكان إنشائه أو إرساله، ووسيلة إنشائه، وارتباطه بسجلات إلكترونية أخرى، بما يضمن فهمه وإثباته والاحتجاج به قانونيًا.
59. **الهجمات السيبرانية:** هي أفعال متعمدة تُنفَّذ عبر الوسائل الرقمية أو الشبكات الإلكترونية بهدف اختراق الأنظمة أو الشبكات أو البيانات أو تعطيلها أو التجسس عليها أو التلاعب بها، بما يؤدي إلى الإضرار بالأمن المعلوماتي أو استمرارية الأعمال أو الخصوصية أو السلامة الرقمية للأفراد والمؤسسات أو الدول.
60. **القانون:** قانون المعاملات الالكترونية رقم (6) لسنة 2022م.
61. **اللائحة:** اللائحة التنفيذية لقانون المعاملات الالكترونية رقم (6) لسنة 2022م.
62. **القانون التجاري:** القانون رقم (23) لسنة 2010م بشأن النشاط التجاري.

الفصل الأول

أحكام عامة

المادة (2): أهداف اللائحة

تهدف هذه اللائحة إلى تحقيق الآتي:

1- تنظيم وحماية المعاملات الإلكترونية.

2- ضمان موثوقية المعاملات الإلكترونية، وتعزيز الثقة العامة في صحتها وسلامتها.

3- حماية الحقوق المترتبة على الاستخدام المشروع لوسائل التقنية الحديثة.

4- تعزيز مبدأ المساواة القانونية بين الوثائق الورقية والإلكترونية من حيث الحجية، والاثبات، والآثار القانونية، وفق القانون.

5. تمكين الجهات الحكومية والخاصة من تقديم خدماتها بوسائل الكترونية، وفق ضوابط قانونية واضحة، بما يسهل التحول إلى الإدارة الإلكترونية.

6- تعزيز التحول الرقمي.

7- تعزيز التجارة الإلكترونية.

8- حماية حقوق المتعاملين إلكترونيا لا سيما في العقود، والخدمات، والتوقيعات، والمعاملات الرقمية للمستهلك الالكتروني.

9- تعزيز الأمان الإلكتروني (السيبراني)، وتحسين جودة الخدمات.

المادة (3): مجال سريان اللائحة

تسري أحكام هذه اللائحة على التصرفات والمعاملات التي تتم بين الأشخاص الطبيعيين والمعنويين بطرق إلكترونية، وعلى السجلات، والتوقيعات الإلكترونية، وخدمات الدفع الالكتروني، والمراسلات الرقمية، وأي معلومات إلكترونية، كما تسري على الخدمات الحكومية عبر الوسائط الإلكترونية، وأنظمة الأرشفة الإلكترونية، وحفظ البيانات، والتزامات مزودي خدمات المعاملات الالكترونية، وشروط الترخيص، والرقابة عليها، وحماية حقوق مستخدمي المعاملات الالكترونية.

المادة (4)

تخضع لأحكام هذه اللائحة المعاملات التي تتم بين أشخاص أتفقوا على إجرائها بطرق إلكترونية، ويجوز استنتاج موافقة الشخص على ذلك من سلوكه كما في الحالات الآتية:

1- إذا جرى العرف أو العادة بين الأطراف على التعامل الإلكتروني.

2- إذا وجد تعامل إلكتروني سابق بين الطرفين اتصل به التعامل الجديد.

3- إذا تمت المراسلات السابقة على العقد بوسائل الكترونية.

4- إذا كان التعامل مع جهة اعتبارية يسمح نظامها الأساسي بالتعامل الإلكتروني.

5. إذا لم يعترض أحد الطرفين صراحة على إبرام التصرف بالطريق الإلكتروني.

6- أي سلوك آخر يستنتج منه نية الأطراف إجراء تعاملهم بوسيلة الكترونية.

المادة (5): حالات مستثناة من الخضوع للائحة

استثناءً من أحكام المادة السابقة لا تسري هذه اللائحة على إنشاء، وإصدار، وتوثيق، وتعديل، المعاملات الآتية:

1- الوصايا وتعديلها.

2- الوقف وتعديل شروطه.

3- التصرفات العقارية التي تتطلب التوثيق الرسمي، وتتعلق بحقوق عينية على عقار.

4- عقود الإيجار الواردة على عقار إذا زادت مدتها على ثلاث سنوات.

5. المسائل المتعلقة بالأحوال الشخصية.

6- إجراءات التقاضي التي تدار حضريا وفق قوانين المرافعات المدنية والإجراءات الجنائية، ما لم ينص القانون صراحة على إمكانية إجرائها إلكترونيا.

7- الوثائق السيادية، أو الأمنية، أو العسكرية، التي لا تجيز الحكومة التعامل بها عبر الوسائط الالكترونية؛ نظرا لسريتها، أو حساسيتها.

8- الإخطارات المتعلقة بفسخ العقود المُبرمة بوسائل غير الإلكترونية، ما لم يتفق الأطراف على خلاف ذلك.

9- أي مستند يوجب القانون توثيقه رسميا.

المادة (6): التزام الحكومة بتشجيع العمل بالوسائل الإلكترونية

مع مراعاة أحكام المادة الثالثة من القانون، تعمل الحكومة على الاعتماد على الوسائل الإلكترونية للقيام بالتصرفات والمعاملات التي تتم بين الأشخاص، وذلك بتقديم التسهيلات والإعفاءات اللازمة لدعم التحول الرقمي في أنشطة القطاع العام والخاص، بما يضمن سرعة الإجراءات، وخفض التكلفة، وتحقيق الشفافية والتنافسية.

المادة (7): قبول الحكومة للتعامل الإلكتروني

مع مراعاة حكم المادة الرابعة من القانون، يجب أن يكون قبول الحكومة للتعامل الإلكتروني صريحاً، وفي جميع الأحوال لا يعد قبولها التعامل بوسائل إلكترونية في معاملة أو تصرف معين قبولاً للتعامل بهذه الوسائل في معاملات أو تصرفات أخرى.

ويعد اعتماد مجلس الوزراء لهذه اللائحة قبولا صريحا من الحكومة للتعامل الالكتروني.

الفصل الثاني

التوقيع الإلكتروني والمحررات الإلكترونية

المادة (8): ضوابط إنشاء التوقيع الإلكتروني

يجوز لأي شخص طبيعي أو معنوي إنشاء توقيع إلكتروني باستخدام منظومة موثوق بها، شريطة الالتزام بالضوابط الآتية:

1- أن تعتمد المنظومة المستخدمة في إنشاء التوقيع على تقنيات تشفير متقدمة تضمن سرية البيانات، وسلامتها من التلاعب أو الاختراق.
2- أن تكون وسيلة التوقيع الإلكتروني صادرة أو معتمدة من الهيئة المختصة، أو من الشركات المرخصة من قبلها.
3- أن يتم التحقق من هوية الموقع وربط بياناته الفنية بالتوقيع الإلكتروني بطريقة آمنة.
4- أن تُظهر وسيلة التوقيع الإلكتروني بوضوح إرادة الموقع في الالتزام بمضمون المحرر الموقع عليه.
5. أن يكون التوقيع مرتبطاً بالمحرر الإلكتروني بشكل تقني يمنع التعديل أو الاستبدال.
6- أن تخضع جميع أدوات التوقيع لاختبارات وضمانات الأمان الفني، والتدقيق الدوري، مع توثيق سجل الاستخدام.
7- أن تكون المنظومة المستخدمة في إنشاء التوقيع مرخصة ومعتمدة وفق المعايير الفنية والأمنية المعتمدة لدى الهيئة.
8- أن يتضمن التوقيع الإلكتروني آلية فنية تُمكن من التحقق من هوية الموقع، وسلامة البيانات المُوقع عليها، ودون الاعتماد على جهة خارجية في حال كان التوقيع ذاتي الإنشاء.

المادة (9): صور التوقيع الإلكتروني

يجوز الاتفاق على استعمال نوع معين من التوقيع إلكتروني **(بسيط/متقدم/مؤمن)**، ويعد هذا التوقيع ملزماً لهم متى توفرت فيه الشروط والضوابط المنصوص عليها في القانون واللائحة.

المادة (10): شروط صحة التوقيع الإلكتروني

يشترط لصحة التوقيع الإلكتروني ما يأتي:
1- أن ينشأ التوقيع عن وسيلة معتمدة.
2- أن يتم التحقق من هوية المستخدم باستخدام شهادة رقمية موثقة.
3- أن تكون جميع بيانات إنشاء التوقيع محفوظة تحت السيطرة الحصرية للمستخدم.
4- أن يتم ربط التوقيع بالمحرر الإلكتروني بواسطة خوارزمية تسمح بكشف أي تعديل.

المادة (11): التزامات صاحب التوقيع الإلكتروني

يلتزم صاحب التوقيع الإلكتروني بالآتي:
1- حماية مفتاحه الخاص ووسائل التوقيع من الوصول أو الاستخدام غير المشروع.
2- إخطار مقدم خدمات التصديق فور علمه أو شكه بوقوع خرق أمني أو اختراق.
3- تزويد جهة مقدم خدمات التصديق بكافة البيانات اللازمة لتعطيل التوقيع، وتحديد الاستخدام غير المشروع.
4- التأكد من صحة بياناته الشخصية عند الحصول على شهادة التصديق.
5. إتباع إجراءات الإخطار المعتمدة من جهة التصديق.

المادة (12): مسؤولية صاحب التوقيع الإلكتروني

يترتب على الاخلال بالوجبات المنصوص عليها في المادة السابقة مسؤولية الشخص عن جميع الاثار الناجمة عن سوء الاستخدام

المادة (13): التثبت صحة التوقيع الإلكتروني

1- **يعد** التوقيع الإلكتروني صالحاً وملزماً أذا تم التثبت من صحته بواسطة شهادة تصديق إلكتروني صادرة عن جهة اعتماد مرخصة، وأمكن من خلاله تحديد هوية الموقع.

2- عند الطعن في صحة التوقيع يتم الاستعانة بالوسائل التقنية وخبرة جهات الاعتماد من نسبة التوقيع للمعني.

3- لا يقبل إنكار الموقع لتوقعيه الإلكتروني متى ثبت أن وسائل التوقيع كانت تحت سيطرته المنفردة.

المادة (14): التوقيع الإلكتروني المنشأ في الخارج

يُعتد بالتوقيع المنشأ خارج ليبيا من جهات معترف بها لدى تلك الدول، إذا وافقت الهيئة على ذلك.

المادة (15): شروط استيفاء شرط الكتابة الإلكترونية

مع عدم الاخلال بحق الهيئة في إضافة شروط أخرى، تعدّ الوثائق، أو المحررات، أو المستندات، أو السجلات، أو البيانات الإلكترونية، مستوفية لشرط الكتابة إذا توفرت فيها الشروط الآتية:

1- إذا تم إنشاؤها، أو إرسالها، أو حفظها، بصيغة إلكترونية معترف بها.

2- إذا أمكن استرجاع محتواها بصيغة قابلة للقراءة.

3- أذا كانت قابلة للحفظ والاستخراج لاحقًا بنفس الحالة التي أنشئت بها، دون تغيير جوهري في محتواها.

وتطبق على هذه المحررات قواعد الإثبات المنصوص عليها في التشريعات النافذة، متى استوفت الشروط الفنية المذكورة.

المادة (16): ضو ابط حفظ المحررات الإلكترونية

عند حفظ المحررات إلكترونيًا، يجب الالتزام بالآتي:

1- اعتماد وسائط حفظ إلكترونية موثوقة، تتيح حفظ البيانات الأصلية كما أُنشئت أو أُرسلت.

2- توفير خاصية البحث، والوصول، والاسترجاع، للبيانات عند الحاجة.

3- الاحتفاظ بسجلات رقمية تؤكد وقت وتاريخ الإنشاء، أو التعديل، أو الوصول للبيانات.

4- أن تكـــون أنظمـــة الحفـــظ مـــزودة بوســـائل الحمايـــة مـــن الحـــذف، أو التلاعـــب، أو الوصـــول غير المصرح به.

وللهيئة في سبيل مواكبة التطورات التقنية أضافة أي شرط أو إجراء تراه لازماً.

المادة (17): شروط الوثيقة الإلكترونية الأصلية

تُعدُّ الوثيقة الإلكترونية «أصلية» في الحالات الآتية:

1- إذا تم إنشاؤها عبر نظام مؤمّن ذي سجل زمني.

2- إذا احتفظت بشكلها النهائي منذ إنشائها الأول، وتم تأمينها من التعديل.

3- إذا أُرفق بها توقيع إلكتروني مؤمَّن، وشهادة رقمية صالحة.

4- إذا أمكن عرض المحتوى كاملاً والتأكد من مطابقته للمحرر الأصلي إلكترونيًا.

5. أي شروط أخرى تقررها الهيئة.

المادة (18): حجية النسخة الورقية والدعامة الإلكترونية

1- تكـــون النســـخة الورقيـــة مـــن المحـــرر الإلكترونـــي حجـــة قانونيـــة إذا ثبتـــت مطابقتهـــا للأصـــل الإلكترونـــي، ويجـــب إرفـــاق النســـخة الورقيـــة بإفـــادة إلكترونيـــة أو خـــتم زمنـــي يؤكـــد صـــحتها ومصدرها.

2- وتكـــون للدعامـــة الإلكترونيـــة (وســـيط التخـــزين) ذات الحجيـــة القانونيـــة مـــا دامـــت مؤمنة، ومتاحة للفحص.

المادة (19): شروط حجية السجلات والرسائل الإلكترونية

مـــع مراعـــاة أحكـــام التشـــريعات النافـــذة، تتمتـــع الســـجلات والرســـائل الإلكترونيـــة بالحجية القانونية للأوراق العرفية متى توفرت فيها الشروط الآتية:

1- استخدام وسيلة إنشاء معتمدة فنيًا.

2- الاعتماد على توقيع إلكتروني آمن.

3- ضمان سلامة المحتوى منذ الإنشاء وحتى الحفظ أو التسليم.

4- إمكانية التحقق من مصدر ومتلقي الرسالة أو السجل.

5. أي شروط أخرى تقررها الهيئة.

المادة (20): شروط نسبة الرسالة الإلكترونية إلى المنشئ

تُعد الرسالة الإلكترونية صادرة عن المنشئ في الحالات الآتية:

1- إذا أرسلها بنفسه باستخدام نظام توقيع شخصي.

2- إذا أرســـلها شـــخص مفـــوض بـــذلك بموجـــب القـــانون، أو الاتفـــاق، أو بواســـطة شـــخص لـــه صلاحية التصرف بحكم عمله.

3- إذا أنشأها نظام معلوماتي مبرمج لصالح المنشئ.

المادة (21): نسبة الرسالة الإلكترونية إلى المرسل إليه

تُعد الرسالة صادرة من المُرسِل ما لم يُخطر المُرسَل إليه بخلاف ذلك خلال وقت معقول تحدده الهيئة، ويجب على المُرسَل إليه بذل العناية اللازمة للتحقق من المصدر باستخدام الإجراءات الفنية، أو الوسائل المتفق عليها.

المادة (22): الإقرار بتسلم الرسالة الإلكترونية

1- إذا اشترط المُرسِل في الرسالة الإلكترونية تلقي إقراراً بتَسلُمها، تُعد الرسالة كأن لم تُرسَل حتى تَسلُم الإقرار.

2- فإذا لم يحدد المُرسِل، أو لم يتم الاتفاق على أن يكون الإقرار المشار إليه وفقاً لشكل معين، جاز الإقرار بتَسلُم الرسالة عن طريق أي اتصال آلي أو وسيلة أخرى، أو أي سلوك من جانب المُرسَل أليه يكون كافياً لإعلام المُرسِل بالتَسلُم.

المادة (23): تحديد وقت بعث الرسالة الإلكترونية

1- تُعد الرسالة الإلكترونية مرسلة من تاريخ خروجها من نطاق سيطرة المنشئ، أو من ينوب عنه في الإرسال، ما لم يوجد اتفاق أو عرف يقضي بخلاف ذلك.

2- يُثبت تحقق هذا الخروج فنياً عن طريق سجل الإرسال الإلكتروني المعتمد، وذلك كله مع مراعاة نص المادة 23 من القانون.

المادة (24): تحديد وقت تسلم الرسالة الإلكترونية

يتحدد وقت تسليم الرسالة الإلكترونية على النحو الاتي:

1- إذا لم يعين المرسل إليه نظاما للمعلومات، يكون تسليم الرسالة الإلكترونية وقت دخولها في نظام معلومات تابع للمرسَل إليه.

2- وفي حالة تعيين المرسل إليه نظام للمعلومات لغرض التسلُم، يكون التسليم في الوقت الذي تدخل فيه الرسالة الإلكترونية إلى ذلك النظام.

3- وإذا دخلت الرسالة إلى نظام معلومات تابع للمرسل إليه بخلاف نظام المعلومات المعين، يكون وقت التسليم هو الوقت الذي يتم فيه استخراج الرسالة الإلكترونية بواسطة المرسل إليه.

المادة (25): تحديد مكان إرسال الرسالة الإلكترونية وتسلمها

يُعتد بمقر العمل الرسمي للمُرسِل والمُرسَل إليه لتحديد مكان الإرسال والاستلام، وفي حال تعدد المقرات، يُعتد بالمقر الأقرب للمعاملة، أو بالمقر الرئيسي، أما إذا لم يوجد مقر عمل، فيُعتد بمحل الإقامة المعتاد لكل منهما.

المادة (26):

لا يُعد إشعار الاستلام دليلاً على مطابقة مضمون الرسالة الإلكترونية للمضمون الأصلي المُرسِل، ويقتصر أثره على أثبات وصول الرسالة إلى نظام أو عنوان المستلم، مالم يثبت العكس بوسائل فنية أو قانونية.

المادة (27): تعدد التوقيعات الإلكترونية على ذات المحرر

في حال وجود أكثر من توقيع إلكتروني على محرر واحد، يجب أن يتضمن كل توقيع ما يلي:

1- اسم الموقع وصفته وتاريخ التوقيع.

2- تسلسل زمني واضح لعملية التوقيع.

3- طريقة فنية تضمن إمكانية التحقق من كل توقيع دون الاخلال بحجيته.

المادة (28): أثر تعديل المحرر الإلكتروني بعد التوقيع

يفقد المحرر الإلكتروني قيمته القانونية أذا تم تعديله إلكترونياً، باستثناء الحالات الاتية:

1- إعادة التوقيع على النسخة المعدلة بالكامل.

2- إضافة توقيع إلكتروني منفصل يقر بالتعديل ويرتبط به فنياً.

3- اعتماد آلية تقنية تظهر بوضوح وقت وطبيعة التعديل والموقع عليه.

المادة (29): توقيع الأطراف ذوي الإعاقة أو المساعدة التقنية

يجوز استخدام تقنيات مساعدة، لتمكين الأشخاص ذوي الإعاقة من إنشاء توقيع إلكتروني، بالشروط الآتية:

1- أن ترتبط التقنية مباشرة بالشخص الموقّع دون تدخل طرف ثالث.

2- أن تكون التقنية معتمدة ضمن المعايير الفنية للهيئة

3- أن يُرفق سجل تقني يوضح طريقة توقيع الشخص صاحب الإعاقة.

4- أن يراعى في ذلك التشريعات ذات الصلة بالمعاقين والقاصرين ومن في حكمهم.

5. أي شروط أخرى تقررها الهيئة.

المادة (30): اللغة والمحتوى في التوقيع الإلكتروني

يجب أن تكون البيانات المرتبطة بالتوقيع الإلكتروني مفهومة، وقابلة للعرض بلغة واضحة، ويراعى قدر الإمكان أن تكون باللغة العربية، أو مرفقة بترجمة معتمدة، إذا تم استخدامها في محررات قانونية.

المادة (31): استخدام التوقيع الإلكتروني في العقود الرسمية

ما لم ينص القانون على خلاف ذلك، لا يجوز استخدام التوقيع الإلكتروني في التصرفات التي يشترط القانون تحريرها في مستند رسمي.

المادة (32): ختم الزمن الإلكتروني

يجب أن تُنفذ عملية ختم الزمن وفق المعايير الأتية:

1- استخدام ساعة زمنية آمنة ومزامنة بشكل مستمر مع مصدر زمني موثوق ومعتمد من الهيئة.

2- إنشاء الختم الزمني باستخدام آلية تشفير رقمي يربط الختم الزمني بالمحرر الإلكتروني أو التوقيع بصورة لا تقبل التعديل أو التنصل منها.

3- الاحتفاظ بسجلات موثقة لجميع عمليات ختم الزمن التي يجريها مزود الخدمة، لمدة لا تقل عن عشر سنوات.

المادة (33): حجية ختم الزمن الإلكتروني

يُعتمد ختم الزمن الإلكتروني دليلاً على:

1- وقت إنشاء، أو إرسال، أو تسلم المحرر الإلكتروني.

2- إثبات وجود المستند، أو التوقيع في لحظة زمنية محددة.

3- حماية المستندات من الادعاءات المتعلقة بتعديلها بعد إنشائها أو توقيعها.

المادة (34): التزامات مزودي خدمة ختم الزمن الإلكتروني

يجب على مزودي خدمات ختم الزمن ما يأتي:

1- الحصول على ترخيص من الهيئة لمزاولة هذا النشاط.

2- الالتزام بالمعايير الفنية والأمنية التي تحددها الهيئة، بما في ذلك استخدام وحدات توقيت محمية.

3- تفعيل آليات تحقق إلكترونية تتيح للأطراف الثالثة التأكد من صحة الختم الزمني، وسلامة ارتباطه بالمحرر الإلكتروني أو التوقيع.

المادة (35): حجية ختم الزمن الإلكتروني الصادر في الخارج

لا يُعتد بختم الزمن الإلكتروني الصادر من أي دولة، ما لم يُعترف به صراحة من الهيئة، أو بموجب اتفاقية اعتراف متبادل.

المادة (36): ختم الزمن الإلكتروني للجهات العامة

يجوز للهيئة اعتماد مزود مركزي لخدمات ختم الزمن لجهات القطاع العام، أو تحديد معايير التشغيل والتكامل بين مزودي الختم وبنية المصادقة الوطنية.

المادة (37): المعايير التقنية لختم الزمن الإلكتروني

تصدر الهيئة دليلاً فنياً يحدد المعايير التقنية لخدمة ختم الزمن، ومن ضمنها: خوارزميات التوقيع الزمني، بنية الطلب والاستجابة، وآليات ومعايير حماية السجلات.

المادة (38): بيانات السجل الإلكتروني

يجب أن يتضمن السجل أو المحرر الإلكتروني البيانات التي تحدد هوية السجل وارتباطه بالتقابل الإلكتروني والسجلات الإلكترونية الأخرى، وتشمل تلك البيانات العناصر التالية:

1- معلومات منشئ السجل الإلكتروني.

2- معلومات مرسل السجل الإلكتروني أذا كان مختلفا عن المنشئ.

3- معلومات المرسل إليه السجل الإلكتروني

4- رقم العملية التي يتضمنها السجل الإلكتروني وطبيعتها.

5. تاريخ انشاء وارسال واستلام السجل الإلكتروني ووقته.

6- معلومات إعادة الارسال، أو التعديل، او الإلغاء، وكذلك رسائل إقرار الاستلام في حالة اشتراط ذلك من قبل المرسل.

المادة (39): ضوابط وآليات استرجاع السجلات والمستندات الإلكترونية

مع عدم الاخلال بالنصوص المتعلقة بحفظ السجل الإلكتروني، يجب عند استرجاع المحررات الإلكترونية والاطلاع عليها التزام بما يأتي:

1- أن تكون السجلات والمستندات الإلكترونية مقروءة، ومفهومة، ومستوفاة، ومتكاملة.

2- أن تكون هناك صيغة إلكترونية متفق عليها أو متعارف على الأخذ بها بين طرفي التعامل الإلكتروني، تضمن توفير المعلومات المتعلقة بالتعامل الإلكتروني.

3- أن يراعى في جميع الحالات التي يتعذر فيها الاطلاع على السجلات الإلكترونية، تطبيق الحلول الفنية المناسبة لتسجيل جميع الحالات التي يتعذر فيها الاطلاع.

المادة (40): المعني بحفظ السجلات الإلكترونية

يحدد بقرار من الهيئة ضوابط تعيين الشخص الملزم بحفظ السجل الإلكتروني.

ويجوز لمن أُلزم بحفظ السجل الإلكتروني الاستعانة بخدمات شخص أو جهة أخرى لاستيفاء شروط الحفظ، دون أن يؤثر ذلك في مسؤوليته.

ويلتزم طرفا التعامل الإلكتروني بحفظ البيانات الالكترونية وخصوصيتها.

المادة (41): المدة الزمنية لحفظ السجلات الإلكترونية.

مع مراعاة التشريعات النافذة، والاتفاقيات، أو العقود المبرمة بين طرفي التعامل الإلكتروني، يحدد بقرار من الهيئة الوطنية لأمن وسلامة المعلومات الحد الأدنى للمدة الزمنية الواجب بقاء السجلات محفوظة خلالها.

المادة (42): شروط حفظ السجلات الإلكترونية

يشترط لحفظ السجلات والبيانات الإلكترونية توفر الشروط الاتية:

1- اتباع قواعد وإجراءات واضحة ومَوثُقة لحفظ السجلات.

2- حفظ السجلات والبيانات الإلكترونية في أي حال بما يتناسب مع النظام المعمول به لدى من قام بالحفظ.

3- تحدد بلائحة خاصة تصدرها الهيئة قواعد سلامة السجلات الإلكترونية وخطط الاستفادة منه.

4- استخدام التقنيات المناسبة لضمان حفظ السجل الإلكتروني بالشكل الذي أنشئ، أو أرسل، أو سُلم به، مع ضمان أن محتواه مطابق للمحتوى الذي أنشئ، أو أرسل، أو سلم به.

المادة (43): حفظ المستندات والرسائل الإلكترونية

يكون حفظ المستندات والمحررات الإلكترونية على النحو الاتي:

1- استخدام نظام إلكتروني موثوق لحفظ الوثائق.

2- أن يكون المستند محفوظًا بطريقة تمنع التعديل غير المصرح به.

3- تصدر الهيئة قرارا بتحديد ضوابط حفظ سجل الأحداث.

المادة (44): حجية الصور المنسوخة

مع مراعاة القوانين النافذة، لا تعد الصور المنسوخة من المحرر الإلكتروني على الورق حجة الا إذا احتوت على رمز تحقق أو توقيع رقمي مستخرج من نظام معتمد.

وفي حال المنازعة، يكون التحقق من صحة الصورة المنسوخة على الورق عن طريق مضاهاتها بالمستند الإلكتروني الأصلي وفق الإجراءات الفنية المعتمدة من الهيئة.

تتولى الهيئة وضع معايير خاصة بالمضاهاة.

المادة (45): تحقق المحكمة من صحة السجل أو الرسالة

عند تقديم مستند رقمي إلى المحكمة يجب بيان الآتي:

1- هوية المرسل.

2- طريقة الارسال والجهة التي أرسلته.

3- الوسيلة المستخدمة لحمايته.

المادة (46): حجية المحرر الإلكتروني

كل محرر أو مراسلة إلكترونية تصدر من البريد الإلكتروني الرسمي للمؤسسة، أو يرسلها أحد موظفيها المكلفين بذلك، تُعد محرراً رسمياً، وحجة قانونية على هذه المؤسسة، دون اشتراط التوقيع اليدوي، طالما ثبتت سلامة مصدرها وصحة نسبتها إلى المؤسسة.

المادة (47): الآثار القانونية المترتبة على المعاملات الإلكترونية

1- تتمتع المعاملات، والسجلات، والوثائق، والتواقيع، الإلكترونية بذات القوة القانونية لنظيراتها الخطية.

2- كل كتابة إلكترونية غير مرتبطة بتوقيع إلكتروني تصدر من الخصم ويكون من شأنها أن تجعل المعاملة الإلكترونية المدعى بها قريبة الاحتمال تعد مبدأ ثبوت بالكتابة.

الفصل الثالث

التصديق الإلكتروني

المادة (48):

1- تقوم الهيئة بوضع واعتماد الضوابط والمعايير الفنية والأمنية اللازمة لعمليات التصديق الإلكتروني، بما في ذلك:

أ- معايير البنية التحتية التقنية لمقدمي خدمات التصديق.

ب- بروتوكولات الأمان وتشفير البيانات.

ج- إجراءات التحقق من الهوية.

د- متطلبات حفظ السجلات والبيانات.

2- تتولى الهيئة وضع الضوابط والمعايير اللازمة لإنشاء، وتشغيل، وتأمين المواقع الإلكترونية الحكومية، وعلى كل الجهات الحكومية الالتزام بها، ويحق للهيئة إلغاء وتعليق التراخيص الممنوحة لهذه المواقع إذا تبين مخالفتها لأحكام هذه اللائحة.

3- تقوم الهيئة بإجراءات التدقيق والمراقبة على مقدمي خدمات التصديق والمواقع الإلكترونية المرخصة، للتأكد من التزامهم بالضوابط والمواصفات المعتمدة.

المادة (49): منح رخص المزاولة لمقدمي خدمات التصديق

تختص الهيئة بما يلي:

1- تحديد الشروط والمستندات اللازمة للحصول على رخصة مزاولة نشاط مقدم خدمات التصديق الإلكتروني.

2- دراسة الطلبات والتحقق من استيفائها للشروط والمتطلبات الفنية والمالية والإدارية والأمنية.

3- إصدار الرخصة بعد سداد الرسوم المقررة، وتحديد مدة سريانها وشروط تجديدها.

المادة (50): التحقق من التزام مقدم خدمات التصديق

يجب على الهيئة القيام بما يلي:

1- وضع آليات للتدقيق والمراجعة الدورية والمراقبة لمقدمي خدمات التصديق الإلكتروني.

2- وضع ضوابط إعداد التقارير الدورية من قبل مقدمي خدمات التصديق الإلكتروني حول أنشطتهم، وذلك للتأكد من مدى التزامهم بالشروط المقررة من قبل الهيئة.

المادة (51): إصداروتسليم وحفظ شهادات المصادقة الإلكترونية

تحدد الهيئة عند قيامها بإصدار الشهادات مباشرة، الإجراءات والمتطلبات اللازمة لذلك.

فإذا تم الإصدار عبر مقدم خدمات تصديق إلكتروني، تضع الهيئة الضوابط التي يجب على مقدم الخدمة اتباعها، بما في ذلك آليات التحقق من هوية طالب الشهادة، ومعايير أمان إصدار الشهادة وحفظها.

المادة (52): ضوابط إصدارشهادة المصادقة الإلكترونية

لا يجوز لمقدم خدمات التصديق الإلكتروني إصدار أي شهادة مصادقة إلكترونية إلا بعد التأكد من الآتي:

1- التحقق الدقيق من هوية طالب الشهادة باستخدام وسائل تحقق موثوقة تحددها الهيئة.

2- التحقق من ملكية المفتاح العام المنسوب لطالب الشهادة.

3- التأكد من سلامة النظام المستخدم لإصدار الشهادة، وخلوّه من نقاط ضعف أمنية تؤثر على سلامة البيانات.

4- الحصول على موافقة مكتوبة أو إلكترونية من طالب الشهادة على إصدارها.

5. إرفاق الشهادة بسياسة استخدام واضحة تبين صلاحياتها ونطاقها الزمني والغرض منها.

المادة (53): بيانات شهادات المصادقة الإلكترونية

يجب أن تتضمن شهادة المصادقة الإلكترونية بحد أدنى ما يلي:

1- رقم تسلسلي فريد للشهادة.

2- اسم الجهة أو الشخص صاحب الشهادة.

3- المفتاح العام المرتبط.

4- فترة الصلاحية.
5- الجهة المصدّرة للشهادة.
6- توقيع الجهة المصدقة.
7- عنوان وموقع سياسة الشهادة.
8- طريقة التحقق اللحظي من حالة الشهادة.

المادة (54): ضوابط تسليم الشهادة

على مقدم الخدمة عند تسليم أي شهادة مصادقة إلكترونية مراعاة الآتي:

1- أن يتم تسليم الشهادة للمستفيد إلكترونيًا عبر قناة مؤمنة، باستخدام وسائل تحقق قوية، مع توثيق عملية التسليم وسجلات أحداثها.

2- أن يتيح آلية للمستفيدين تمكنهم من الاطلاع على شهاداتهم إلكترونيًا والتأكد من حالة الشهادة وصلاحيتها وبياناتها.

3- أن يزود المستفيد بنسخة من الشهادة فور إصدارها، مع بيان يوضح حقوقه والتزاماته.

4- أي ضوابط أو شروط أخرى تحددها الهيئة.

المادة (55): ضوابط حفظ الشهادات وسجلاتها

يجب على مقدم الخدمة أن يقوم بحفظ نسخة إلكترونية من كل شهادة مصادقة صادرة، ومن السجلات المرتبطة بها، لمدة لا تقل عن خمس (5) سنوات من تاريخ انتهاء أو إلغاء الشهادة، على أن تشمل السجلات الواجب حفظها ما يلي:

1- طلب إصدار الشهادة.
2- بيانات التحقق من الهوية.
3- نسخة من الشهادة.
4- سجل التعديلات.
5- قرارات الإلغاء أو التعليق.
6- سجلات التحقق الفني المرتبطة بها.

المادة (56): ضوابط حفظ وتخزين السجلات

على مقدم الخدمة أن يراعي في حفظ وتخزين السجلات الضوابط الآتية:

1- أن تحفظ هذه السجلات في بيئة إلكترونية مؤمنة تعتمد التشفير والتوقيع الزمني وإمكانية التتبع.

2- أن تُخزَّن السجلات على خوادم مؤمنة في ليبيا، أو في بيئة سحابية مرخص لها من الهيئة.

3- أي ضوابط وشروط أخرى تحددها الهيئة.

المادة (57): ضوابط قائمة الشهادات الملغاة والمعلقة

يلتزم مقدم الخدمة عند إبطال أو تعليق الشهادات بالضوابط الآتية:

1- إنشاء وتحديث قائمة إبطال وتعليق الشهادات، أو تفعيل خدمة الاستعلام اللحظي على مدار الساعة.

2- تحديث قائمة إبطال وتعليق الشهادات فورًا خلال مدة لا تتجاوز ستين (60) دقيقة من قرار الإلغاء أو التعليق.

3- يجب أن تكون هذه القائمة متاحة للعامة من خلال بوابة إلكترونية، أو عبر واجهة برمجة التطبيقات، مخصص للتحقق الفوري.

4- أي ضوابط وشروط أخرى تحددها الهيئة.

المادة (58): ضوابط التصحيح والإلغاء

تصحح وتلغى شهادات التصديق الإلكتروني وفق الضوابط الآتية:

1- يجوز للمستفيد طلب تصحيح الشهادة خلال فترة صلاحيتها بشرط تقديم اثبات رسمي.

كما يجوز لمقدم الخدمة إلغاء أو تعليق الشهادة في أي من الحالات الآتية:

أ- فقدان السيطرة على المفتاح الخاص.

ب- تقديم بيانات مزيفة.

ج- طلب رسمي من السلطات المختصة.

هـ- بناء على طلب المستفيد.

2- للهيئة إضافة أي حالات أو ضوابط أخرى.

3- على مقدم الخدمة توثيق كل إجراء إلغاء أو تعليق، مع تحديث سجل الشهادة فوراً.

المادة (59): استيراد أو الترخيص باستيراد أدوات التشفير

تتولى الهيئة وضع إطار تنظيمي لاستخدام تقنيات التشفير الوظيفي والخاص، وبما يحقق التوازن بين متطلبات العمل ومقتضيات الأمن الوطني، وذلك على النحو الآتي:

1- تُعدّ الهيئة قائمة محدثة بأدوات وتقنيات التشفير –سواء التشفير الوظيفي المستخدم في الأنشطة المؤسسية أم التشفير الخاص– التي يستلزم استيرادها أو تداولها الحصول على ترخيص مسبق.

2- تُقدَّم طلبات الحصول على الترخيص إلى الهيئة، مرفقةً بالمبررات الداعية لاستخدام التشفير، وبيان الغرض الوظيفي أو الخاص منه، فضلا عن المواصفات الفنية العامة للأدوات المطلوب ترخيصها، دون المساس بمتطلبات السلامة أو الضوابط القانونية.

3- تراعي الهيئة عدم تعارض الاستخدام المصرَّح به مع متطلبات الأمن الوطني أو النظام العام وعليها التحقق من وسائل وبرمجيات وإجراءات مقدمي الخدمة.

المادة (60): المعايير الأمنية

1- تعتمد الهيئة قائمة بالمعايير اللازمة للوسائل والبرمجيات والإجراءات الأمنية، استئناساً إلى المعايير الدولية.

2- على مقدمي الخدمة تقديم ما يثبت التزامهم بهذه المعايير بشكل دوري أو عند الطلب.

المادة (61): منح الرخص للمو اقع الإلكترونية ومر اقبتها

1- تحدد الهيئة فئات المواقع الإلكترونية التي تتطلب ترخيصاً.

2- تقدم طلبات الترخيص للمواقع وفقاً للنماذج والمستندات التي تحددها الهيئة.

3- تراقب الهيئة محتوى وعمل المواقع المرخصة للتأكد من عدم مخالفتها للنظام العام، والقوانين واللوائح والقرارات والاتفاقيات الدولية المصادق عليها من دولة ليبيا.

المادة (62): شروط مزاولة نشاط مقدم خدمات التصديق الإلكتروني

لا يجوز لأي شخص طبيعي أو معنوي مزاولة نشاط تقديم خدمات التصديق الإلكتروني إلا وفق الشروط الآتية:

1- إعداد دراسة جدوى فنية ومالية تثبت قدرته على تقديم الخدمة وفقاً للمعايير المعتمدة من الهيئة.

2- الحصول على ترخيص من الهيئة.

3- المحافظة على سريان صلاحية هذا الترخيص.

المادة (63): الشروط المرعية في طالب الترخيص.

للحصول على رخصة مزاولة نشاط مقدم خدمات التصديق الإلكتروني، يجب على الشخص الطبيعي أو الممثل القانوني للشخص الاعتباري تقديم المستندات الثبوتية التالية للهيئة:

1- لإثبات الجنسية والإقامة: إفادة من مصلحة الجوزات والجنسية، وما يفيد الإقامة الفعلية في ليبيا.

2- لإثبات التمتع بالحقوق المدنية: إفادة من النيابة العامة.

3- لإثبات عدم صدور حكم ضده بشهر الإفلاس: إفادة من السجل التجاري.

4- لإثبات المؤهل العلمي :إحضار أصل المؤهل من شهادة الماجستير في تقنية المعلومات أو ما يعادلها، معتمدة من مركز ضمان الجودة.

5. لإثبات عدم مزاولة نشاط آخر :إفادة من وزارة العمل والتأهيل، وللهيئة التحقق من ذلك.

6- في حال كان طالب الترخيص شركة، يجب تقديم مستخرج حديث من السجل التجاري، وعقد التأسيس أو النظام الأساسي للشركة، فضلا عن استيفائه للشروط المذكورة أعلاه.

المادة (64): إصداروتسليم وحفظ الشهادات

يلتـــزم كـــل مقـــدم خدمـــة تصـــديق إلكترونـــي معتمـــد بإعـــداد كـــراس الشـــروط الخـــاص بنشـــاطه وفـــق المعـــايير المحـــددة فـــي القـــانون واللائحـــة، وذلـــك قبـــل الشـــروع فـــي تقـــديم أي خدمـــة تصـــديق، علـــى أن تتـــولى الهيئـــة اعتمـــاده وفـــق مـــا تضـــعه مـــن معـــايير، وعلـــى أن يـــتم تحـــديث كـــراس الشـــروط كلمـــا طـــرأ تعـــديل جـــوهري علـــى نشـــاط مقـــدم الخدمـــة أو منظومـــات التقنية أو السياسة التشغيلية.

المادة (65): محتويات كراس الشروط

فـــي مقـــام تطبيـــق أحكـــام المـــادة (32) مـــن القـــانون، يجـــب أن يتضـــمن كـــراس الشـــروط الذي يقدمه مقدم خدمات التصديق للهيئة كحد أدنى ما يلي:

1- البيانات التعريفية بمقدم الخدمة، وتراخيص مزاولته للنشاط.

2- الوصـــف الفنـــي لمنظومـــة إنشـــاء وإدارة الشـــهادات الإلكترونيـــة، وإجـــراءات حمايـــة ســـرية وسلامة مفاتيح التشفير.

3- سياسات وإجراءات التحقق من هوية طالبي الشهادات الإلكترونية.

4- شروط إصدار، وتعليق، وإلغاء الشهادات، وإجراءات إخطار المستفيدين بذلك.

5. التزامات مقدم الخدمة تجاه المستفيدين وحدود مسؤوليته القانونية والتقنية.

6- تدابير حماية البيانات الشخصية وسجلات التصديق، ومدة الاحتفاظ بها.

7- آليات تلقي الشكاوى ومعالجتها، وطرق الطعن في القرارات.

8- خطـــة اســـتمرارية الخدمـــة، وإجـــراءات الإخطـــار المســـبق عنـــد التوقـــف الكلـــي أو الجزئـــي أو نقل النشاط.

المادة (66): وسائل موثوق بها لإصداروحفظ الشهادات

يجب على مقدمي خدمات التصديق ومديري المواقع الإلكترونية الالتزام بالآتي:

1- اســـتخدام أنظمـــة تشـــفير معتمـــدة مـــن الهيئـــة، أو متوافقـــة مـــع المعـــايير الدوليـــة المعتـــرف بها من الهيئة.

2- تطبيـــق إجـــراءات أمنيـــة صـــارمة للـــتحكم فـــي الوصـــول إلـــى أنظمـــة إصـــدار وحفـــظ الشـــهادات، بمـــا فـــي ذلـــك اســـتخدام كلمـــات مـــرور قويـــة، والمصـــادقة متعـــددة العوامـــل، وتسجيل كافة عمليات الوصول.

3- إجراء اختبارات اختراق دورية للأنظمة، للتأكد من خلوها من الثغرات الأمنية.

وعلـــى الهيئـــة تحديـــد معـــايير الوســـائل الموثـــوق بهـــا ومتطلبـــات الحمايـــة مـــن التزويـــر وفـــق أحكام في المادة (37) من القانون.

المادة (67): السجل الإلكتروني لشهادات المصادقة

تحـــدد الهيئـــة الشـــروط والإجـــراءات اللازمـــة للحصـــول علـــى تـــرخيص تقـــديم خـــدمات التصـــديق، وبشـــكل خـــاص مـــدة التـــرخيص، وأحكـــام تجديـــده، ووقفـــه، وإلغـــاؤه، والتنـــازل عنه، والتزامات المرخص له.

المادة (68):

مـــع مراعـــاة شـــروط التـــرخيص الصـــادرة عـــن الهيئـــة، يجـــب أن يتـــوفر لـــدى المتقـــدم بطلب الترخيص لتقديم خدمات التصديق الإلكتروني ما يلي:

1- منظومـــة بيانـــات إلكترونيـــة، ومنظومـــة لشـــهادات التصـــديق الإلكترونـــي وللتواقيـــع الإلكترونيـــة، ضـــمن بيئـــة عمـــل فنيـــة قياســـية، لا تقـــل عـــن المســـتوى الأمني للمعـــايير المحـــددة مـــن الهيئـــة، حســـبما يـــرد فـــي سياســـة الشـــهادة الرقميـــة وإجـــراءات التصـــديق الإلكترونـــي، وفقـــاً للضوابط التالية:

أ- عـــدم قابليـــة الاســـتنتاج، او الاســـتنباط للمفـــاتيح الخاصـــة أو البيانـــات المكونـــة للتوقيـــع الإلكتروني

ب- الحفـــاظ علـــى ســـرية البيانـــات، وحمايتهـــا مـــن التلـــف أو التزويـــر أو الاختـــراق، وفـــق المستوى الأمني المحدد من الهيئة.

2- بنيـــة تحتيـــة فنيـــة، ومـــوارد إداريـــة علـــى درجـــة عاليـــة مـــن الكفـــاءة والمعياريـــة، بمســـتوى لا يقـــل عـــن المقـــاييس المعتمـــدة مـــن الهيئـــة، لتشـــغيل وإدارة جميـــع عمليـــات التصـــديق الرقمـــي التي من أهمها:

أ- إصدار شهادات التصديق، وما يتبع ذلك من تجديدها، وتعليقها وإلغائها وإعادتها.

ب- إدارة عمليـــات التشـــفير ومـــا يتبعهـــا مـــن حفـــظ للمفتـــاح الخـــاص بمقـــدم خـــدمات التصديق، وكذلك المفاتيح العامة.

3- إتاحـــة البيانـــات الخاصـــة بـــالتحقق مـــن صـــحة الشـــهادات، والتواقيـــع الإلكترونيـــة لجميـــع أطراف التعامل الإلكتروني، مع ضمان ربطها مباشرة بقوائم الشهادات الموقوفة والملغاة.

4- تأســـيس جميـــع المـــوارد الإلكترونيـــة وتشـــغيلها وإدارتهـــا، وفـــق آليـــة تضـــمن عمليـــات الحفـــظ والارشـــفة، وكـــذلك النقـــل إلـــى منظومـــات وقواعـــد بيانـــات قياســـية أخـــرى، مـــع تـــوفير البـــدائل والخطط التي بموجبها يتم ضمان استمرار الخدمة.

المادة (69): جمع المعلومات لإصدار الشهادة

يحظر على مقدم الخدمة ما يلي:

1- جمع أي بيانات لا تكون ضرورية للتحقق من هوية الطالب وإصدار الشهادة.

2- جمع أي معلومة شخصية من الغير دون موافقة كتابية أو إلكترونية صريحة.

وعلـــى مقـــدم الخدمـــة توضـــيح الغـــرض مـــن جمـــع كـــل معلومـــة، وبيـــان كيفيـــة اســـتخدامها وحمايتها.

المادة (70): بيانات شهادة المصادقة

1- تحـــدد الهيئـــة بقـــرار منهـــا الشـــروط التفصـــيلية للســـلامة والأمـــان الواجـــب توفرهـــا فـــي شهادات المصادقة.

2- بالإضـــافة إلـــى البيانـــات المـــذكورة فـــي المـــادة (36) مـــن القـــانون، يجـــوز أن تتضـــمن الشـــهادة بناءً على طلب صاحبها أو متطلبات الهيئة ما يلي:

أ- حـــدود اســـتخدام الشـــهادة (كتحديـــد طبيعـــة الاســـتخدام شخصـــي أم تجـــاري، مطلـــق أم مقيد بسقف مالي).

ب- الرقم التسلسلي الفريد للشهادة.

ج- الخوارزميات المستخدمة في التوقيع والتشفير.

3- يجـــب أن تكـــون آليـــة التحقـــق مـــن رقـــم الهويـــة للشـــخص الطبيعـــي، ورقـــم الســـجل التجـــاري والضريبي للشخص الاعتباري معتمدة وموثقة.

المادة (71): التزام مقدم الخدمة بضمان صحة البيانات

1- لضمان صحة المعلومات الواردة في الشهادة، يجب على مقدم الخدمة:

أ- تطبيق إجراءات تحقق صارمة من هوية طالب الشهادة والمستندات المقدمة.

ب- استخدام مصادر موثوقة للتحقق من البيانات.

2- لضمان العلاقة بين صاحب الشهادة ومنظومة التدقيق، يجب على مقدم الخدمة:

أ- التأكد من أن المفتاح الخاص المرتبط بالشهادة تحت سيطرة صاحب الشهادة وحده.

ب- توفير إرشادات واضحة لصاحب الشهادة حول كيفية حماية مفتاحه الخاص.

3- لضـــمان اســـتقلال صـــاحب الشـــهادة بمســـك منظومـــة إنشـــاء التوقيـــع، يجـــب علـــى مقـــدم الخدمة:

أ- عدم الاحتفاظ بنسخة من المفتاح الخاص لصاحب الشهادة.

ب- التأكـــد مـــن أن الأدوات أو البرمجيـــات المســـتخدمة لإنشـــاء التوقيـــع الإلكترونـــي تتوافـــق مع الضوابط الفنية والتقنية المحددة من الهيئة.

المادة (72): التدقيق في هوية ممثل الشخص الاعتباري

1- عنـــد تقـــدم شـــخص طبيعـــي بطلـــب شـــهادة مصـــادقة نيابـــة عـــن شـــخص اعتبـــاري، يجـــب على مقدم الخدمة التحقق مما يلي:

أ- هوية الشخص الطبيعي المتقدم بالطلب.

ب- صـــفته القانونيـــة فـــي تمثيـــل الشـــخص الاعتبـــاري (كتفـــويض رســـمي، أو مســـتخرج مـــن السجل التجاري يبين المخولين بالتوقيع).

ج- صحة وجود الشخص الاعتباري ونشاطه.

2- يجـــب علـــى مقـــدم خـــدمات التصـــديق، عنـــد تســـليم شـــهادة المصـــادقة إلـــى شـــخص اعتبـــاري التدقيق في هوية الشخص الطبيعي الذي يتقدم إليه، وفي تمثيله للشخص الاعتباري.

المادة (73): ضوابط تعليق وإلغاء الشهادات

يلتزم مقدم الخدمة عند تعليق أو إلغاء شهادات التصديق بما يلي:

1- عند طلب صاحب الشهادة تعليقها، يجب على مقدم الخدمة الاستجابة فوراً وتوثيق الطلب.

2- في الحالات الأخرى المذكورة في المادة (39)، يقوم مقدم الخدمة بالتحقيق الفوري، وعند ثبوت أي من هذه الحالات يعلق الشهادة.

3- يتم إبلاغ صاحب الشهادة بالتعليق وسببه كتابياً أو إلكترونياً خلال أربع وعشرين (24) ساعة كحد اقصى من التعليق.

4- يتم نشر حالة "معلقة" للشهادة في السجل الإلكتروني فوراً.

هـ لصاحب الشهادة أو للغير من ذوي المصلحة الطعن في قرار التعليق لدى الهيئة خلال خمسة عشر (15) يوماً كحد اقصى من تاريخ النشر في السجل، وتبت الهيئة في الطعن خلال ثلاثين (30) يوماً.

5- يتم رفع التعليق فور زوال سببه وتأكيد صحة المعلومات واستخدامها الشرعي، ويتم تحديث حالة الشهادة في السجل.

المادة (74): إلغاء شهادة التصديق

1- يجوز إلغاء شهادة التصديق الإلكتروني، أو إيقاف العمل بها بناء على طلب صاحبها، دون أن يؤثر ذلك على حقوق أي من الأطراف الذين سبق لهم التعامل بموجب الشهادة الملغاة أو الموقوفة.

2- يجب على مقدم خدمات التصديق الإلكتروني إيقاف الشهادة أو إلغاءها بناء على أمر من الهيئة، أو من أي جهة أخرى مختصة، ويعد مقدم خدمات التصديق بناءً على ذلك مسؤولاً عن إكمال الإجراءات التالية:

أ- تنفيذ ما ورد في أمر الإلغاء أو الإيقاف.

ب- إشعار صاحب الشهادة بالإجراءات التي تمت.

ج- تنبيه كل من يعتمد على الشهادة مستقبلاً عبر مقدم خدمات التصديق بعدم صلاحيتها وفقاً لإجراءات التصديق الرقمي، والقواعد والإجراءات المنظمة لعمل الهيئة.

3- يجب على الهيئة في حال قيامها بإيقاف الترخيص أو إلغائه، إعطاء مقدم خدمات التصديق الوقت الكافي للتقيد بالقرار، وتتخذ الهيئة الترتيبات اللازمة لضمان استمرار تقديم الخدمات للمستخدمين.

المادة (75): حالات إلغاء الشهادة

على مقدم خدمات التصديق الإلكتروني إلغاء الشهادة فوراً، في الحالات الآتية:

1- بناءً على طلب صاحب الشهادة.

ب- فور إبلاغه بوفاة الشخص الطبيعي، أو انقضاء الشخص المعنوي صاحب الشهادة.

2- إذا تبين بالفحص بعد تعليق الشهادة أن المعلومات الواردة بها غير صحيحة، أو مزورة، أو أنها غير مطابقة للواقع، أو أنه قد تم انتهاك منظومة إنشاء التوقيع، أو استعمال الشهادة للتدليس.

3- يجوز لصاحب الشهادة، أو الغير الطعن في قرار مقدم الخدمات الخاص بإلغاء الشهادة خلال ثلاثين (30) يوما من تاريخ نشره بالسجل الإلكتروني المنصوص عليه في القانون، ويقدم الطعن أمام المحكمة الابتدائية التي يوجد في دائرة اختصاصها موطن مقدم خدمات التصديق الإلكتروني.

المادة (76): التزامات ومسؤوليات صاحب الشهادة

1- يلتزم صاحب شهادة التصديق الإلكتروني بما يلي:

أ- المحافظة على سرية مفاتيحه الخاصة، وعدم تمكين الغير من الاطلاع عليها أو استخدامها.

ب- الإبلاغ الفوري للجهة المصدرة عند فقدان وسيلة التوقيع الإلكتروني، أو الاشتباه في اختراقها، وذلك لطلب تعليق أو ألغاء الشهادة.

2- يعد كل توقيع إلكتروني صادرا بواسطة المفتاح الخاص المرتبط بالشهادة صحيحاً وملزماً لصاحبه، مالم يثبت فقد السيطرة عليه، وكان قد أخطر الجهة المصدرة بذلك فور علمه.

3- يتحمل صاحب الشهادة المسؤولية المدنية عن أي ضرر يلحق بالغير نتيجة إهماله أو تأخره في الإبلاغ عن فقدان أو اختراق مفتاحه الخاص.

4- لا يسأل صاحب الشهادة عن أي استعمال غير مشروع لشهادته إذا ثبت قيامه بواجباته في المحافظة والإبلاغ وفق احكام هذا القانون.

وعلى الهيئة وضع آلية للتحقق من عدم استخدام عناصر تشفير لشهادات معلقة أو ملغاة لدى مقدم خدمة آخر، وذلك بالتنسيق بين مقدمي الخدمات، أو من خلال قاعدة بيانات مركزية تشرف عليها الهيئة.

المادة (77): التزامات مقدم خدمات التصديق الإلكتروني

يلتزم مقدم خدمات التصديق الإلكتروني بما يلي:

1- التحقق من هوية طالب الشهادة، والتأكد من صحة البيانات التي تتضمنها، وذلك وفق الضوابط الفنية والقانونية المقررة.

2- اتخاذ التدابير الفنية والتنظيمية الكفيلة بحماية أنظمته من الاختراق أو التلاعب، وضمان سلامة إصدار الشهادات، وحفظها، وإلغائها، أو تعليقها.

3- إتاحة خدمة التحقق من حالة الشهادة (صالحة، معلقة، ملغاة) للجمهور بوسيلة تقنية مأمونة ومستمرة.

4- حفظ السجلات والمعلومات المتعلقة بالشهادات الإلكترونية، والعمليات المرتبطة بها لمدة لا تقل عن المدة التي يحددها القانون، وبما يتيح الرجوع إليها عند الحاجة القضائية أو الإدارية.

المادة (78): مسؤوليات مقدم خدمات التصديق الإلكتروني

1- يتحمل مقدم خدمات التصديق الإلكتروني المسؤولية عن الأضرار التي تلحق بالغير نتيجة إهماله أو تقصيره في التحقق من هوية طالب الشهادة، وفي إتاحة المعلومات الخاصة بحالة الشهادة، وحماية أنظمته من الاختراق.

2- على أن مقدم خدمات التصديق الإلكتروني لا يسأل عن الأضرار الناشئة عن استعمال صاحب الشهادة لشهادته بما يخالف أغراضها، أو عن تقصير صاحب الشهادة في واجباته بالمحافظة على مفاتيحه الخاصة أو الإبلاغ عن فقدها.

المادة (79) : الاعتراف بالشهادات الأجنبية

1- تقوم الهيئة بتقييم مدى تكافؤ معايير وإجراءات التصديق الإلكتروني في الدول الأخرى مع المعايير المطبقة في ليبيا كأساس لإبرام اتفاقيات الاعتراف المتبادل.

2- تحدد الهيئة إجراءات وقواعد الاعتراف بالشهادات الصادرة من مقدمي خدمات التصديق إلكتروني في دول ترتبط مع ليبيا باتفاقيات اعتراف متبادل.

3- تحتفظ الهيئة بسجل لمقدمي خدمات التصديق الأجانب المعتمدين والشهادات المعترف بها.

المادة (80): إيقاف نشاط مقدم خدمات التصديق الإلكتروني

1- لا يجوز لمقدم خدمات التصديق الالكتروني إيقاف نشاطه كليًا أو جزئيًا إلا بعد الحصول على موافقة الجهة المختصة، والإعلان عن ذلك بوسيلة مأمونة وعلنية.

2- يجب على مقدم خدمات التصديق الالكتروني إخطار أصحاب الشهادات الصادرة عنه قبل مدة لا تقل عن ستين (60) يومًا من تاريخ الإيقاف، مع بيان الإجراءات المتخذة لضمان استمرار صلاحية أو إلغاء الشهادات.

3- تلتزم الجهة المختصة باتخاذ ما يلزم لضمان حماية مصالح أصحاب الشهادات، بما في ذلك نقل إدارة الشهادات إلى مقدم خدمات آخر مرخص له.

المادة (81): تحويل نشاط مقدم خدمات التصديق الإلكتروني

1- يجوز لمقدم خدمات التصديق الالكتروني تحويل نشاطه إلى مقدم خدمات تصديق الكتروني آخر، وذلك بمراعاة الشروط الآتية:

أ- الحصول على موافقة الجهة المختصة.

ب- ضمان استمرار الخدمات دون انقطاع.

ج- نقل جميع السجلات والبيانات الخاصة بالشهادات بأمان.

2- على أنه وفي سائر الأحوال يبقى مقدم خدمات التصديق الالكتروني الأصلي مسؤولاً عن أي التزامات أو أضرار نشأت قبل تاريخ التحويل، ما لم يتفق على غير ذلك بإذن الجهة المختصة.

3- تلتزم الجهة المختصة بالإشراف على عملية التحويل لضمان عدم المساس بمصالح أصحاب الشهادات والمتعاملين.

الفصل الرابع

المعاملات الإلكترونية

المادة (82): التعبير عن نية التعاقد الإلكتروني

يجوز لأغراض التعاقد، التعبير عن الإيجاب والقبول –كليا أو جزئيا– بوسائل إلكترونية، ويعد هذا التعبير ملزما للأطراف متى تم التوقيع عليه إلكترونيا بما يوافق أحكام القانون واللائحة.

المادة (83):

1- يجوز إبرام العقد بين وسائط إلكترونية آلية معدة ومبرمجة مسبقا للقيام بذلك، كما يجوز إبرامه بين وسيط إلكتروني آلي مملوك لشخص طبيعي أو معنوي وبين شخص طبيعي أو معنوي متى كان هذا الشخص يعلم أو من المفترض أن يعلم أنه يتعامل مع وسيط إلكتروني آلي سيتولى مهمة إبرام العقد أو تنفيذه.

2- ويكون للعقود الإلكترونية ذات الآثار القانونية للعقود التي تبرم وفق القواعد العامة.

التزامات البائع

المادة (84): الالتزام بالإعلام

يلتزم البائع قبل إبرام العقد مع المستهلك بأن يوفر له المعلومات الآتية:

1- اسم البائع أو مقدم الخدمة، وعنوانه، ورقم هاتفه، وبريده الإلكتروني.

2- مراحل إنجاز المعاملة التجارية بالتفصيل.

3- طبيعة ومواصفات وسعر المنتج أو الخدمة.

4- نفقات تسليم المنتج، ومبلغ تأمينه، وأي نفقات أخرى.

5- الفترة التي يكون خلالها المنتج معروضاً بالأسعار المحددة.

6- شروط الضمانات التجارية، وخدمات ما بعد البيع.

7- طرق وإجراءات الدفع.

8- طرق وأجال تنفيذ العقد، ومكان التسليم، والآثار المترتبة على عدم تنفيذ الالتزام.

9- إمكانية العدول عن الشراء وآجاله.

10- كيفية اقرار الصفقة.
11- طرق إرجاع المنتج، أو استبداله، وإرجاع المبلغ، وآجاله.
12- نفقات استعمال تقنيات الاتصال حين يتم احتسابها على أساس مختلف عن التعرفة الجاري العمل بها.
13- شروط فسخ العقد إذا كان لمدة غير محددة، أو لمدة تزيد على السنة.
14- الحد الأدنى لمدة العقد فيما يخص العقود المتعلقة بتزويد المستهلك بمنتج أو خدمة خلال مدة طويلة أو بصفة دورية.
15- يجب توفير هذه المعلومات إلكترونياً ووضعها في متناول المستهلك للاطلاع عليها خلال مراحل المعاملة جميعها.

المادة (85):

1- يلتزم البائع بأن يوفر للمستهلك –عند الطلب– خلال عشرة (10) أيام من إبرام العقد رسالة خطية أو إلكترونية تتضمن المعلومات المتعلقة بعملية البيع.
2- كما يلتزم البائع بأن يوفر للمستهلك أثناء مرحلتي إبرام العقد وتنفيذه خدمة إلكترونية تتيح له مكنة التواصل المباشر مع البائع.

المادة (86): التزامات البائع في البيع بالتجربة

1- إذا نص البيع على شرط تجربة المنتج أو الخدمة، التزم البائع بتحمل الأضرار التي قد يتعرض لها المنتج أو الخدمة، وذلك حتى انتهاء مدة التجربة باستثناء حالات سوء الاستعمال من قبل المستهلك.
2- يقع باطلا كل شرط يقضي بخلاف ذلك.

المادة (87):التزامات البائع عند الاخلال بالعقد

1- إذا تعذر على البائع توفير المنتج أو الخدمة المطلوبة من المستهلك، وجب عليه إبلاغه بذلك قبل حلول التاريخ المحدد في العقد للتسليم بأربع وعشرين (24) ساعة، وإرجاع المبلغ المدفوع كاملاً.
2- يتم الإبلاغ بإرسال إخطار إلكتروني للمستهلك، ويعد العقد في هذه الحالة مفسوخا من تلقاء نفسه دون حاجة إلى حكم أو إعذار.

التزامات البائع عند إلغاء العقد

المادة (88): توفير أيقونة خاصة بالإلغاء

1- يلتزم البائع في الحالات التي يجوز فيها للمستهلك إلغاء العقد بأن يوفر له أيقونة إلكترونية تحت عنوان "إلغاء عقدك" أو أي صيغة مماثلة، مكتوبة بحروف واضحة، يمكن الولوج إليها بسهولة وبشكل مباشر عبر أي وسيط إلكتروني تم من خلاله العقد.

2- إذا كان إلغاء العقد مشروطاً، يجب أن تشير أيقونة الإلغاء بشكل واضح ومفهوم إلى المعلومات المتعلقة بشروط الإلغاء، بما في ذلك -عند الاقتضاء- وجود مهلة للإخطار، وتبعات الإلغاء.

المادة (89): حالات خاصة من الإلغاء

لغرض تحديد العقد المستهدف بالإلغاء، يجوز في الحالات التي تتطلب فيها طبيعة العقد ذلك أن تقود ايقونة الإلغاء المنصوص عليها في المادة السابقة قبل إنتاج أثرها في إلغاء العقد إلى خانة تتضمن بيانات يضيفها المستهلك، تزود البائع بمعلومات عن هوية المستهلك، كعنوانه الإلكتروني أو البريدي الذي يسمح للبائع بتأكيد استلامه لإشعار الإنهاء، وتاريخ إلغاء العقد.

المادة (90): الإخطار بالإلغاء

يجب أن يسمح النظام الإلكتروني الخاص بإلغاء العقد بأن يدخل المستهلك إلى نافذة يعرض من خلالها ملخص لما قام بإضافته من بيانات وفق المادة السابقة، وتسمح له بأن يراجع تلك البيانات أو يعدل فيها إن لزم الأمر، ثم يقوم المستهلك بإخطار البائع بإنهاء العقد بواسطة تفعيل ايقونة الإلغاء التي يصل إليها مباشرة من خلال الصفحة المذكورة.

المادة (91): حالات لا يجوز فيها للمستهلك إلغاء العقد

استثناء من أحكام المواد السابقة، ومع مراعاة المادة (18) من قانون المعاملات الإلكترونية، وفي غير حالات العيوب الظاهرة أو الخفية، لا يجوز للمستهلك إلغاء العقد في الحالات التالية:

1- إذا طلب المستهلك توفير الخدمة قبل انتهاء مدة العدول عن الشراء، ووفر له البائع ذلك.

2- إذا تم تزويد المستهلك بمنتجات حسب مواصفات شخصية، أو تزويده بمنتوجات لا يمكن إعادة إرسالها، أو تكون قابلة للتلف، أو الهلاك، أو الفساد، لانتهاء مدة صلاحيتها.

3- إذا قام المستهلك بنزع الأختام عن التسجيلات السمعية أو البصرية، أو البرمجيات والمواد الإعلامية.

4- شراء الكتب والصحف والمجلات.

مادة (92): الغاء العقد المرتبط بقرض

إذا كانت عملية الشراء ناتجة كلياً أو جزئياً عن قرض ممنوح للمستهلك من قبل البائع أو غيره على أساس عقد مبرم بين البائع وغير المستهلك، فإن إلغاء المستهلك لعقد البيع يؤدي إلى فسخ عقد القرض من دون تعويض.

المادة (93): فسخ العقد بسبب إخلال البائع بالتزاماته

يُفسخ العقد إذا أخل البائع بالتزاماته، ويسترجع المستهلك المبلغ المدفوع، مع احتفاظه بحقه في التعويض إن كان له مقتضى، ما لم يكن الضرر ناتجاً عن قوة قاهرة.

زمان ومكان العقد

المادة (94): زمان الإبرام ومكانه

يكون زمان ومكان انعقاد العقد هو زمان ومكان استلام الرسالة الإلكترونية بقبول الإيجاب، ما لم يوجد اتفاق أو عرف يقضي بغير ذلك.

المادة (95): زمان التنفيذ ومكانه

1- يجب على البائع أن ينفذ العقد بتسليم المنتج أو الخدمة للمستهلك في موطنه خلال ثلاثين (30) يوما من تاريخ إبرام العقد، ما لم يوجد اتفاق أو عرف يقضي بغير ذلك.

2- إذا تعذر على البائع توفير المنتج أو الخدمة خلال الميعاد المذكور، أو في المكان المتفق عليه، أو الذي يحدده العرف، التزم بإبلاغ المستهلك قبل انقضاء هذا الميعاد بأربع وعشرين (24) ساعة، مع إرجاع المبلغ المدفوع كاملاً إلى صاحبه.

المادة (96): عبء الإثبات

1- إذا فرض القانون توفير معلومات معينة، أو مراعاة آجال أو شروط محددة، أو الحصول على موافقات، وقع عبء إثبات ذلك على البائع.

2- كما يقع على البائع عند المنازعة إثبات أنه أوفى بجميع التزاماته المنصوص عليها في قانون المعاملات الإلكترونية وهذه اللائحة.

3- يعد باطلاً كل اتفاق يقضي بخلاف ما تقدم.

المادة (97): القانون الواجب التطبيق على العقد

1- تخضع العقود الإلكترونية التي يتم إبرامها وتنفيذها في ليبيا لأحكام قانون المعاملات الإلكترونية وهذه واللائحة.

2- على أنه إذا تضمن العقد الإلكتروني عنصرا أجنبيا وجب على البائع أن يبين فيه القانون الواجب التطبيق عليه. ولا يجوز في سائر الأحوال أن يتعارض قانون العقد مع قواعد آمرة في القانون الليبي.

الفصل الخامس

حماية المعاملات الإلكترونية

المادة (98):

يستخدم التشفير لحماية المعاملات الإلكترونية بهدف المحافظة على سرية المعلومات، أو البيانات التي تحويها الرسالة الإلكترونية، والتحقق من شخصية المنشئ، ومنع غيره من التقاط المعلومات، أو الرسائل الإلكترونية، بغرض منع وصولها إلى المرسل إليه، أو تشويهها.

مادة (99): طرق حماية نظم المعلومات

تستخدم الطرق الآتية لحماية نظم المعلومات:

1- التشفير بطرق نظم المعلومات.

2- الجدران النارية.

3- مرشحات المعلومات.

4- مجموعة الوسائل المتعلقة بمنع الإنكار.

5. تقنيات التشفير المعطيات والملفات.

6- إجراءات حماية نسخ الحفظ الاحتياطية.

7- البرامج المضادة للفيروسات الإلكترونية.

8- فريق الاستجابة للحوادث السيبرانية.

9- أي طريقة أخرى تحددها اللائحة التنفيذية.

المادة (100): طلب فحص المعلومات

باستثناء مفاتيح التشفير المتعلقة بالأمن الوطني، يجوز للموظف الذي تحدده الهيئة العامة للمصادقة أن يطلب من صاحب أي مفتاح تشفير، تمكينه من فحص المعلومات الضرورية المتعلقة بذلك المفتاح، وعلى صاحب ذلك المفتاح تمكينه من الفحص.

المادة (101): نظام التطبيق والالتزام

1- على جميع الجهات العامة والخاصة التي تنشئ أو تستلم أو تعالج أو تحفظ معاملات إلكترونية أن تبذل العناية اللازمة لتأمين هذه المعاملات بما في ذلك الضوابط الأمنية والتنظيمية المنصوص عليها في هذه اللائحة.

2- تتولى الهيئة وضع الأطر المرجعية والمعايير الفنية والتشغيلية والاعتماد الدوري لضوابط هذا الفصل وتحديثها، بما يراعي أفضل الممارسات الدولية.

المادة (102): الحوكمة والمسؤوليات

تلتزم كل جهة بالآتي:

1- استحداث وحدة إدارية متخصصة في إدارة أمن المعلومات تتبع الإدارة العليا مباشرة، ويُعيّن فيها مسؤول أمن المعلومات الذي يتولى إدارة مهام الأمن السيبراني، والامتثال، وإدارة المخاطر المعلوماتية، وذلك بالتنسيق المباشر مع الهيئة.

2- اعتماد سياسة أمن معلومات شاملة، وسياسة حماية بيانات، وإطار إدارة دوري، وخطة استمرارية أعمال وتعافي من الكوارث، مرتبطة بزمن استعادة ونقطة استعادة معتمدين.

المادة (103): المراقبة والقدرات التشغيلية

تلتزم كل جهة بالآتي:

1- إنشاء مركز عمليات أمنية أو من خلال مزود مرخّص؛ يراقب الأنظمة وقنوات المعاملات على مدار الساعة

2- استخدام أنظمة إدارة معلومات وأحداث الأمن ومنظومات تحليل سلوك المستخدم لكشف الانحرافات والسلوكيات عالية المخاطر.

3- تفعيل آليات تسجيل مركزية غير قابلة للعبث مع ختم زمني، وحفظ السجلات لفترة لا تقل عن اثني عشر (12) شهراً، أو حسب ما تقره الهيئة.

المادة (104): استطلاع التهديدات

تعتمد كل جهة مصادر موثوقة لجمع المعلومات والتحريات الاستباقية عن التهديدات، على ان تتشارك عند الاقتضاء هذه التحريات في شبكات تبادل المعلومات القطاعية وتتكامل تقنياً عبر معايير تبادل المؤشرات المعتمد من الهيئة.

المادة (105): الاستجابة للحوادث الأمنية

على كل جهة أن:

1- تعتمد خطة استجابة للحوادث تتضمن أدواراً ومسؤوليات واضحة، ومستويات شدة الحوادث المعتمدة لدى الهيئة، ومستويات خدمة زمنية محددة لكل مستوى.

2- تخطر الهيئة بأي حادث مؤثر على سرية أو سلامة أو توفر المعاملات الإلكترونية خلال أربع وعشرين (24) ساعة من الاكتشاف، مع إعداد تقرير أولي، وتقرير نهائي خلال عشرة (10) أيام عمل يتضمن الأسباب الجذرية والإجراءات التصحيحية.

3- على أن تشمل خطوات الاستجابة: الاكتشاف، الاحتواء، الاستئصال، والاستعادة، والتحقق مما بعد الاستعادة، والدروس المستفادة، مع حفظ الأدلة الرقمية وفق إجراءات سلسلة حضانة الأدلة المعتمدة من الهيئة.

المادة (106): الضوابط الوقائية والتقنية

يجب على كل جهة تطبيق كل أدوات، وتقنيات، وآليات، وإجراءات، الأمن السيبراني التي يتطلبها تحليل المخاطر، الذي يجري حسب المنهجية المعتمدة من الهيئة، وعلى حد أدنى استخدام الضوابط الآتية:

1- المصادقة المتعددة العوامل، وإدارة الهوية، والوصول، وفق المبدأ منح الأقل صلاحيات، وتجزئة الشبكات، ونموذج انعدام الثقة على الأنظمة الحرجة للمعاملات.
2- التشفير الإلزامي للبيانات أثناء النقل والتخزين، وإدارة مفاتيح تشفير خاضعة للرقابة داخل وحدات أمن عتاد مادي عند الاقتضاء.
3- تأمين التطبيقات وواجهات البرمجة، وقيود لمعدلات الإدخال، والتحقق من المدخلات، واختبارات أمنية دورية قبل إطلاق التطبيقات وبعده.
4- إدارة الثغرات والتصحيح الأمني وفق دورة حياة معلنة: تقييم دوري (شهري كحد أدنى)، ومعالجة عاجلة للثغرات الحرجة خلال مدة لا تتجاوز خمسة عشر (15) يوماً، والمتوسطة خلال ثلاثين (30) يوماً، مالم تقرر الهيئة خلاف ذلك.
5- حماية نقاط النهاية والأجهزة المحمولة بتطبيقات مضادة للبرمجيات الخبيثة، مع تفعيل العزل التلقائي عند الاشتباه.
6- استخدام آليات منع تسرب البيانات على قنوات البريد، والتخزين السحابي، والأجهزة المحمولة، وفق سياسات تصنيف المعلومات.
7- النسخ الاحتياطي الدوري غير القابل للتغيير، وفحوصات استعادة دورية.

المادة (107): مراقبة الطرفيات والأطراف الثالثة وسلسة التوريد

1- تجرى تقييمات أمنية قبل التعاقد، ومعاودة التقييم دورياً لمزودي الخدمات السحابية ومُعالجي البيانات والأطراف الثالثة.
2- تُضمن الضوابط الأمنية ومتطلبات الإخطار بالحوادث حقوق وبنود إنهاء آمن للبيانات في العقود المبرمة مع كل الأطراف الأخرى.

المادة (108): الاختبارات والتأكد المستقل

على كل جهة القيام بالإجراءات التالية:

1- اختبارات اختراق نصف سنوية على الأنظمة الحرجة، وتمارين فرق الاختراق في مواجهة فرق الحماية عند الاقتضاء.

2- تمـــارين تقيـــيم جاهزيـــة إجـــراءات الحوكمـــة لمحاكـــاة الأزمـــات تجـــرى ربـــع ســـنوية، تغطـــي مخـــاطر مختلفـــة وعلـــى الأقـــل انتشـــار فيـــروس الفديـــة، وانقطـــاع الخدمـــة، وتســـريب البيانات، وتلف قاعدة المعلومات.

3- تـــدقيق امتثـــال ســـنوي بواســـطة جهـــة معتمـــدة مـــن الهيئـــة، وتقـــديم تقريـــرا إلـــى الهيئـــة خـــلال ثلاثين (30) يوماً من صدوره.

المادة (109): مؤشرات الأداء والمخاطر والتقارير

على كل جهة القيام بما يلي:

1- اعتمـــاد حزمـــة مؤشـــرات يمكـــن عبرهـــا تقيـــيم أداء الأمـــن الســـيبراني بالجهـــة وبشـــكل خـــاص: متوســـط وقـــت الاكتشـــاف، ومتوســـط وقـــت الاســـتجابة، ومعـــدل الحـــوادث ذات الأثـــر العـــالي، ونسبة التصحيحات ضمن المهل، تغطية السجلات، ونسبة الاختبارات المكتملة.

2- أعداد تقارير سنوية للهيئة تتضمن مؤشرات الأداء.

الفصل السادس

(العمليات المصرفية)

المادة (110): الالتزام بالمعايير الملائمة للأمن السيبراني

تلتـــزم المصـــارف والمؤسســـات الماليـــة بالمعـــايير المحليـــة للأمـــن الســـيبراني المعتمـــدة مـــن الهيئة، وعلى الأخص ما يأتي:

1- المعايير الدولية للأمن السيبراني.

2- تبني منظومات أمن معلومات متقدمة، وأنظمة اكتشاف ومنع الاختراقات.

3- تحـــديث الأنظمـــة الأمنيـــة بصـــورة دوريـــة، وتقيـــيم المخـــاطر التقنيـــة وفـــق معـــايير دوليـــة معتمدة.

4- وضـــع خطـــط اســـتمرارية الأعمـــال والتعـــافي مـــن الكـــوارث، وإبـــلاغ مصـــرف ليبيـــا المركـــزي والهيئة فور وقوع أي اختراق أو حادث سيبراني.

5. الامتثال للسياسات الوطنية لأمن وسلامة المعلومات المعتمدة من الهيئة.

المادة (111): العقود المنظمة للعلاقة مع العملاء

يجـــب أن تُحـــرر العقـــود المنظمـــة للخـــدمات المصـــرفية الإلكترونيـــة بلغـــة واضـــحة ودقيقة، وأن تتضمن على وجه الخصوص الآتي:

1- بيانًا مفصلًا بحقوق والتزامات كل طرف.

2- تحديد العمولات، والمصاريف، وأسعار الصرف، بطريقة شفافة.

3- شـــروط وقيـــود تنفيـــذ الأوامـــر، وآليـــات الاعتـــراض والـــتظلم، بمراعـــاة أحكـــام القـــانون واللائحة.

4- مُدد تنفيذ العمليات، ومدى إمكانية إلغائها أو تعديلها.
5. بيان حدود مسؤولية العميل قبل الإبلاغ عن الفقدان أو السرقة.
6- التزام المصرف أو المؤسسة المالية بتصحيح الأخطاء وتعويض الأضرار الناتجة عن خطئه أو تقصيره.
7- وضع آليات مناسبة تمكن العميل من الإبلاغ عن الفقد أو السرقة أو الاختراق.
8- يمكن للعميل إيقاف البطاقة أو الخدمة المصرفية أو المالية في أي وقت ولأي سبب يراه.

المادة (112): الشفافية والعلانية

على المصارف والمؤسسات المالية الالتزام بالآتي:
1- نشر الشروط والأحكام الكاملة، وقيمة الرسوم والعمولات، في مكان ظاهر بفروعها وعلى مواقعها الإلكترونية وتطبيقاتها الرسمية.
2- تبليغ العملاء بأي تعديل جوهري في الشروط أو الرسوم قبل خمسة عشر يوماً من تاريخ نفاذه، بإحدى الوسائل الموثوقة إلكترونياً.
3- يُحظر تحصيل أيّ رسوم أو عمولات غير منصوص عليها صراحةً في العقد المبرم مع العميل.

المادة (113): آليات الاعتراض والتظلم وتسوية النزاعات

يحقّ للعميل الاعتراض أو التظلم على أي عملية مصرفية إلكترونية يعتقد بعدم صحتها، وذلك خلال أجل لا يتجاوز ثلاثين (30) يوماً من تاريخ علمه بها.

المادة (114): حماية البيانات والخصوصية

على المصارف والمؤسسات المالية الالتزام باتخاذ كافة التدابير والإجراءات لحماية البيانات والخصوصية وذلك بمراعاة الآتي:
1- الحفاظ التام على سرية بيانات العملاء ومعلوماتهم، وعدم الإفصاح عنها إلا بموافقة كتابية صريحة من العميل أو بناءً على أمر قضائي، أو لسبب يقرُّه القانون.
2- اتخاذ تدابير تقنية وتنظيمية تحول دون معالجة أو تخزين أو نقل البيانات خارج الأطر القانونية المحددة.

المادة (115): إصدار واستعمال البطاقات المصرفية

تُسلم البطاقات المصرفية للعملاء مرفقةً بمعلومات التعريف، بعد توثيق استلامها وتأكيد العلم بمخاطر استعمالها، على أن تلتزم المصارف والمؤسسات المالية بتوفير وسائل آمنة وفورية للإبلاغ عن فقدان البطاقة أو سرقتها، ويترتب على الإبلاغ إيقاف التعامل بالبطاقة فوراً دون تحميل العميل أي رسوم، ويتحمل المصرف أو المؤسسة المالية المسؤولية الكاملة عن العمليات بعد تاريخ الإبلاغ.

المادة (116): الإلغاء والتعديل والرجوع في أوامر الدفع

1- يجوز للعميل إلغاء أو تعديل أمر الدفع الإلكتروني طالما لم يُنفذ، على أن يلتزم المصرف في العقد بتحديد المدة الزمنية المتاحة للإلغاء أو التعديل.

2- في حال التنفيذ الجزئي، يجوز للعميل إيقاف تنفيذ الجزء غير المنفذ من العملية، إذا كانت التجزئة ممكنة.

المادة (117): النقود الإلكترونية وإصدارها

تصدر النقود الإلكترونية حصرياً من مصارف أو مؤسسات مالية مرخص لها بذلك. ويُبين في العقد خصائص النقود الإلكترونية، وآلية إعادة استرداد قيمتها، ومدى قبولها لدى التجار والجهات الأخرى، وفقًا للضوابط التي يعتمدها مصرف ليبيا المركزي.

المادة (118): التوعية

تلتزم المصارف بإعداد برامج توعية حول مزايا ومخاطر الدفع الإلكتروني، وبنشر إرشادات الأمن السيبراني على المواقع الإلكترونية والتطبيقات بشكل دوري، وبتعريف العملاء بحقوقهم وسبل حمايتها.

المادة (119): المسؤولية في حالة الهجمات السيبرانية

تضع المصارف الخطط اللازمة لتفادي وقوع الهجمات السيبرانية، والتعامل معها في حالة وقوعها في الوقت المناسب، ومعالجة آثارها، وتلتزم بتعويض العملاء عن الاضرار المباشرة الناتجة عن أي اهمال أو تقصير في أنظمة الحماية.

المادة (120): الالتزام المؤسسي بالدفع الإلكتروني

1- تلتزم الحكومة والجهات التابعة لها، وغيرها من الجهات المستقلة والشركات العامة والخاصة، باعتماد الدفع الإلكتروني كوسيلة حصريّة في سداد كافة التزاماتها المالية المستحقة عليها، بما في ذلك رواتب وأجور العاملين، والمشتريات، والمقاولات، وأي التزامات مالية أخرى.

2- ويكون الدفع الإلكتروني هو الخيار الأساسي المعتمد لقبول سداد الديون والرسوم والضرائب والغرامات والعمولات وجميع الإيرادات والمدفوعات والتحويلات المالية المستحقّة لصالح الدولة والجهات التابعة لها، مع مراعاة ما قد تقتضيه طبيعة بعض التعاملات من استثناءات.

وذلك بمراعاة الالتزام بالمحافظة على التوازن بين الحفاظ على أمن البيانات، وحماية الخصوصية والشفافية، ومكافحة غسل الأموال وتمويل الإرهاب.

المادة (121): الصكوك الإلكترونية

1- تُعـــدّ الصـــكوك الإلكترونيـــة محـــرّرات مصـــرفية تُنشـــأ وتُوقَّـــع إلكترونيـــاً عبـــر الأنظمـــة المعتمَدة لدى المصارف التجارية، ووفقًا للضوابط التي يُصدرها مصرف ليبيا المركزي.

2- يجـــب أن تتضـــمن الصـــكوك الإلكترونيـــة البيانـــات الإلزاميـــة المقـــررة فـــي القـــانون التجـــاري، بمـــا فـــي ذلـــك التوقيـــع الإلكترونـــي وفقًـــا لأحكـــام قـــانون المعـــاملات الإلكترونيـــة ولائحتـــه التنفيذية.

3- يجـــب حفـــظ الصـــكوك الإلكترونيـــة فـــي قواعـــد بيانـــات آمنـــة، تتـــيح للجهـــات المختصـــة الاطلاع على صورها الرقمية عند الاقتضاء.

4- تُقـــدَّم الصـــكوك الإلكترونيـــة للتحصـــيل أو الوفـــاء إلكترونيـــاً عبـــر آليـــات النظـــام المصـــرفي للدفع، مع مراعاة قواعد المقاصة الإلكترونية المنظمة لذلك.

5- لا يجـــوز إصـــدار صـــك إلكترونـــي مـــا لـــم يكـــن للســـاحب حســـاب مصـــرفي نشـــط يغطـــي قيمتـــه عند الإصدار.

المادة (122): السفتجة الإلكترونية

1- تُنشـــأ الســـفتجة الإلكترونيـــة وتُحـــرَّر باســـتخدام وســـائط إلكترونيـــة معتمَـــدة وفـــق النمـــوذج القياسي الذي يصدره المصرف المركزي.

2- يجـــب أن تتضـــمن الســـفتجة الإلكترونيـــة البيانـــات الجوهريـــة المنصـــوص عليهـــا فـــي القـــانون التجـــاري، ويُعتـــد بـــالتوقيع الإلكترونـــي وفقـــا لأحكـــام قـــانون المعـــاملات الإلكترونيـــة ولائحتـــه التنفيذية، وتكون له ذات القيمة القانونية للتوقيع اليدوي.

3- يجـــب حفـــظ الســـفتجة الإلكترونيـــة ضـــمن ســـجلات إلكترونيـــة آمنـــة ومشـــفّرة، مـــع تمكـــين ذوي الشأن من الاطلاع على نسخة إلكترونية منها متى طلبوا ذلك.

4- يجـــوز تـــداول الســـفتجة الإلكترونيـــة بالتـــدوير الإلكترونـــي، كمـــا يجـــوز قبولهـــا مـــن المســـحوب عليـــه، وفقًـــا للضـــوابط التـــي تصـــدرها الهيئـــة، شـــريطة اســـتعمال توقيـــع إلكترونـــي معتمد عند إجراء التدوير أو القبول.

5- وفـــي حالـــة عـــدم الوفـــاء، تُنفَّـــذ الســـفتجة الإلكترونيـــة بـــذات الآليـــات والإجـــراءات المقـــررة قانونًا للسفتجة الورقية.

مادة (123): السند الإذني الإلكتروني

1- ينشـــأ الســـند الإذنـــي الإلكترونـــي باســـتخدام وســـائط إلكترونيـــة معتمَـــدة، وفـــق نمـــوذج قياسي تصدره الهيئة، وبما يتفق مع الضوابط المقررة بالقانون.

2- يجـــب أن يتضـــمن الســـند الإذنـــي الإلكترونـــي البيانـــات الجوهريـــة المنصـــوص عليهـــا فـــي القـــانون التجـــاري، ويُعتـــد بـــالتوقيع الإلكترونـــي وفقـــا لأحكـــام قـــانون المعـــاملات الإلكترونيـــة ولائحتـــه التنفيذيـــة باعتبـــاره منتِجًـــا لجميـــع الآثـــار القانونيـــة المترتبـــة علـــى التوقيـــع اليـــدوي فـــي السندات الإذنية الورقية.

3- يُحفظ السند الإذني الإلكتروني ضمن سجلات إلكترونية آمنة ومشفَّرة، مع تمكين ذوي الشأن من الاطلاع على نسخة إلكترونية منه متى طلبوا ذلك.
4- يجوز تداول السند الإذني الإلكتروني بالتدوير الإلكتروني وفقًا للضوابط التي تضعها الهيئة، مع وجوب استعمال توقيع إلكتروني معتمد للتدوير.
5- وفي حالة عدم الوفاء، تُطبَّق في تنفيذ السند الأذني الإلكتروني ذات الإجراءات القانونية المقررة للسندات الإذنية الورقية.

الفصل السابع
حماية البيانات الخاصة
جمع البيانات

المادة (124): أهداف نظام حماية البيانات

تهدف أحكام هذا الفصل إلى وضع الضوابط والشروط والإجراءات التنظيمية اللازمة لتنفيذ نظام حماية البيانات المقدمة إلى مقدمي خدمات التصديق الإلكتروني، وذلك بما يضمن الشفافية والعدالة في معالجة البيانات ويعزز الثقة في المعاملات ويحقق التوازن بين المصالح المشروعة، ويكفل حقوق الأفراد في حماية خصوصيتهم.

المادة (125): ضوابط جمع البيانات

1- لا يجوز لمقدمي خدمات التصديق الإلكتروني جمع البيانات الخاصة، أو معالجتها، أو الإفصاح عنها، أو إفشائها بأي وسيلة من الوسائل، إلا بموافقة صريحة وواضحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا، وفي الحدود اللازمة لأداء الخدمة.
2- ويجب أن يكون جمع البيانات الشخصية أو معالجتها في الحد الأدنى من البيانات الضرورية لغرض إصدار شهادة التصديق الإلكتروني أو المحافظة عليها أو تسهيل ذلك.

المادة (126): الموافقة على جمع البيانات ومعالجتها

تثبت موافقة الشخص على جمع أو معالجة بياته الخاصة بأحد الوسائل الآتية:
1- التوقيع، سواء كان ورقيا حضوريا أم إلكترونياً عن بعد.
2- التطبيقات الرقمية القائمة على المصادقة البيومترية، والمعتمدة من الهيئة للتحقق من الهوية، شريطة ألّا يترتب على استخدامها تسجيل أو تخزين دائم للبيانات البيومترية، ويُكتفى بعملية التحقق اللحظي، أو بالوسائل البديلة التي تعتمدها الهيئة.
3- أي وسيلة أخرى تحددها الهيئة.

المادة (127): توثيق المو افقة وسحبها

1- يجب توثيق جميع وسائل الموافقة المستخدمة، وأن تكون الموافقة منفصلة عن أي شروط أو بنود أخرى، مع وجوب إعلام صاحب البيانات بحقه في سحب الموافقة في أي وقت، وأن سحب الموافقة لا يؤثر على شرعية التعاملات التي تمت قبل السحب.

2- في حال سحب الموافقة، يجب على مقدم خدمة التصديق الإلكتروني التوقف عن معالجة البيانات التي تستند إلى هذه الموافقة مع مراعاة أي شروط قانونية تفرض الاحتفاظ بالبيانات.

المادة (128): جمع البيانات دون مو افقة

استثناء من أحكام المواد السابقة، يكون الحصول على البيانات الشخصية، أو الإفصاح عنها، أو توفيرها، أو معالجتها، مشروعا إذا كانت:

1- ضرورية لغرض منع، أو كشف، جريمة بناءً على طلب رسمي من جهات التحقيق.

2- مطلوبة، أو مصرحا بها، بموجب قانون أو أمر من المحكمة.

3- ضرورية لتقدير أو تحصيل أي ضريبة أو رسوم.

4- ضرورية لحماية الحياة أو السلامة الشخصية.

5- في الحالات الأخرى التي ينص عليها القانون صراحة لمقتضيات المصلحة العامة أو الأمن القومي، مع الالتزام بالضمانات والتدابير الكفيلة بحماية البيانات.

المادة (129): شروط جمع البيانات ومعالجتها والاحتفاظ بها

يجب على مقدمي خدمات التصديق الإلكتروني الالتزام أثناء جمع البيانات الشخصية، ومعالجتها، والاحتفاظ بها بالشروط الآتية

1- أن تجمع البيانات الشخصية في الحدود التي يتطلبها منح المعني خدمة التصديق الإلكتروني.

2- أن تكون صحيحة، وسليمة، ومؤمنة.

3- أن تعالج بطريقة مشروعة، وملائمة، الأغراض التي جمعت من أجلها.

4- ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.

المادة (130): حق النفاذ إلى البيانات

على مقدمي خدمات التصديق الإلكتروني تمكين الشخص الذي جمعت عنه بيانات شخصية من النفاذ إليها، ويشمل هذا الحق الدخول إلى مواقع البيانات الخاصة المتعلقة بذلك الشخص لغرض الاطلاع عليها، أو تقديم طلب بتصحيحها، أو بتعديلها، أو بتحديثها، أو بنقلها لجهة أخرى، أو بسحب الموافقة المسبقة على معالجتها، وله تخصيص المعالجة في نطاق محدد، وطلب محو البيانات أو طلب إخفائها، وله الاعتراض على المعالجة والتشخيص إذا كانا غير ضروريين لتحقيق الأغراض التي جمعت من أجلها البيانات.

المادة (131): آلية تقنية للنفاذ إلى البيانات

يجب على مقدمي خدمات التصديق الإلكتروني توفير آلية تقنية واضحة وميسرة لصاحب البيانات لطلب القيام بالعمليات المذكورة في المادة السابقة بطريقة إلكترونية، ويجب عليه الاستجابة لهذا الطلب في غضون يومي عمل من تاريخ تسلم الطلب، مالم تطرأ ظروف استثنائية تستدعي تمديد هذا الأجل، وفي جميع الأحوال يجب إعلام صاحب البيانات بسبب التأخير والمدة المتوقعة للاستجابة، مع توثيق العملية في النظام الإلكتروني.

المادة (132): ضمان سرية البيانات

مع مراعاة المادة الخامسة، يلتزم مقدم خدمات التصديق الإلكتروني باتباع الإجراءات المناسبة لضمان سرية البيانات الشخصية التي في عهدته في سياق القيام بوجباته، ولا يجوز له إفشاء، أو تحويل، أو إعلان، أو نشر، تلك البيانات لأي غرض مهما كان، إلا بموافقة مسبقة من الشخص الذي جمعت عنه البيانات أو أمر صادر عن جهة قضائية.

المادة (133): نموذج جمع البيانات

على مقدمي خدمات التصديق الإلكتروني إعداد نموذج لجمع البيانات يتضمن نوعها، والغرض من جمعها، وبيان مدى كونها إلزامية أم اختيارية، ويجب توثيق الجمع عبر سجلات إلكترونية غير قابلة للتعديل بعد التسجيل تحتوي على:

1- الغرض من جمع البيانات.

2- اسم المسؤول عن جمع البيانات.

3- وصف للبيانات التي يتم جمعها.

4- توقيع صاحب البيانات.

5. تاريخ ووقت جمع البيانات.

6- قناة جمع البيانات.

المادة (134): طرق جمع البيانات

يتم جمع البيانات عن طريق:

1- الحضور الشخصي لصاحب البيانات، أو حضور من ينوب عنه، أو من له الولاية الشرعية عليه، أو الممثل القانوني له، ومن غير وجود وسيط، لمقر مؤسسة التصديق الإلكتروني أو أحد فروعها.

2- البوابة الإلكترونية للمؤسسة.

3- البريد الإلكتروني الموثق.

مع تحديد وسيلة تواصل مع مسؤول البيانات لأي طلب متعلق بالبيانات، على ان تكون وسائل التواصل الإلكتروني أمنة وموثوقة.

معالجة البيانات:

المادة (135): ضوابط معالجة البيانات

يجب على مقدمي خدمات التصديق الإلكتروني الالتزام بالضوابط الآتية عند معالجة البيانات:

1- أن تكون جميع عمليات معالجة البيانات الشخصية، والمالية عادلة، وشفافة، وقانونية.

2- أن تتم المعالجة لأغراض محددة، ومشروعة.

3- أن لا تتعدى المعالجة الغرض الذي جمعت من أجله البيانات.

4- يجب الحفاظ على دقة البيانات.

5. يجب دعم حماية معالجة البيانات بشكل استباقي، بدءاً من مراحل تصميم النظم، مرورا بالتطوير وكذلك الخدمات.

المادة (136): التزام مقدمي الخدمات بالإخطار

يلتزم مقدمو خدمات التصديق الإلكتروني، عند إجراء أي تعديل أو تحديث على أنظمتهم أو بنيتهم التقنية أو برامجهم التشغيلية، بإخطار الهيئة مسبقًا أو فور إجرائه، وتقديم تقرير تفصيلي يوضح أثر ذلك التعديل أو التحديث على مستوى حماية وأمان البيانات الشخصية.

المادة (137): الالتزام بضوابط الخصوصية الإدارية

يجب على مقدمي خدمات التصديق الإلكتروني تطبيق ضوابط الخصوصية الإدارية ومن ذلك:

1- سياسة تصنيف البيانات.

2- سياسية خصوصية البيانات.

3- سياسة معالجة البيانات.

4- سياسة إدارة الوصول.

5. سياسة التشفير.

6- سياسة إدارة الثغرات.

7- سياسة الاستجابة للحوادث الأمنية.

8- سياسة الاحتفاظ بالمعلومات والإتلاف الآمن.

تخزين البيانات

المادة (138): حفظ البيانات

يجب أن تكون البيانات الشخصية محفوظة داخل الدولة الليبية لدى مؤسسات التصديق الإلكتروني المعتمدة من قبل الهيئة، وتحت إشراف أمني معلوماتي متكامل، ويلتزم بأعلى معايير الأمن السيبراني، وحماية البيانات وفق الشروط التي تحددها الهيئة.

المادة (139): تحويل البيانات للخارج

إذا تطلب الأمر تحويل البيانات الشخصية إلى خارج ليبيا يجب مراعاة المستوى المناسب من الحماية وعلى الأخص:

1- طبيعة البيانات الشخصية.

2- مصدر المعلومات المضمنة في البيانات.

3- الأغراض المراد معالجة البيانات من أجلها ومدتها.

4- الدولة التي يتم تحويل البيانات إليها والتزاماتها الدولية والقانون المطبق فيها.

5. القواعد ذات الصلة في هذه الدولة.

6- الإجراءات الأمنية المتخذة لحماية البيانات في هذه الدولة.

المادة (140): تشفير البيانات

يجب على مقدمي خدمات التصديق الإلكتروني تطبيق التشفير المتقدم، وإدارة مفاتيح التشفير بشكل مستقل، وتطبيق تقنيات التشفير على كل الأنظمة التي تحتوي على البيانات، وخاصة قواعد البيانات الخاصة بمقدم خدمات التصديق، ويكون التشفير دائما سواء عند التخزين، أو نقل البيانات، ولا يسمح بوجود مفاتيح التشفير في نفس المكان الذي توجد به البيانات.

إدارة حوادث البيانات

المادة (141): اعتماد سياسة وخطة لإدارة حوادث البيانات

يجب على مقدمي خدمات التصديق الإلكتروني أن يعتمدوا سياسة وخطة خاصة بإدارة حوادث البيانات، تشتمل على كل الإجراءات التي يجب القيام بها عند حصول أي حادث طارئ، على أن تشمل إجراءات الكشف عن الحوادث والتحقق منها، وإجراءات الاحتواء والتخفيف من الآثار، وإجراءات التحقيق في سبب الحادث، وإجراءات التعافي، ووضع تدابير وقائية لمنع تكرار ذلك.

المادة (142): الإبلاغ عن حوادث البيانات

يجب على مقدمي خدمات التصديق الإلكتروني إبلاغ الهيئة عند حدوث أي تسريب أو وصول غير مشروع للبيانات خلال أربع وعشرين (24) ساعة من وقوع

الحادث، مع إشعار صاحب البيانات في حالة حدوث تسريب، أو تلف، أو وصول غير مشروع لبياناته.

وإذا كان من شأن حدوث أي مما سبق أن يرتب ضرراً جسيماً على بياناته أو على نفسه وجب إبلاغه فوراً، وتوثيق جميع الحوادث والإجراءات التصحيحية.

ويجب أن يتضمن الإبلاغ طبيعة الخرق الأمني، والفئات والأنواع من البيانات المتأثرة، والعواقب المحتملة للخرق الأمني، والإجراءات المتخذة أو المقترح اتخاذها للمعالجة أو التخفيف من آثار الخرق الأمني.

حذف و إتلاف البيانات

المادة (143): طلب حذف أو إتلاف البيانات

يتم حذف أو إتلاف البيانات بناءً على طلب من صاحب البيانات أو من مسؤول البيانات لدى جهة التصديق الإلكتروني، وذلك بعد التحقق من انتهاء الغرض من الاحتفاظ وبما لا يتعارض مع القانون.

المادة (144): قيود على إتلاف البيانات

يجب على مقدمي خدمات التصديق الالكتروني استخدام وسائل الاتلاف التقني الآمن، ويوثق تاريخ الإتلاف، ونوع البيانات المتلفة، والمسؤول عن العملية في سجل خاص.

المادة (145): قيود إضافية عامة

يلتزم مقدمو خدمات التصديق الإلكتروني، عند إجراء أي تعديل أو تحديث على أنظمتهم، أو بنيتهم التقنية، أو برامجهم التشغيلية، بإخطار الهيئة مسبقًا أو فور إجرائه، وتقديم تقرير تفصيلي يوضح أثر ذلك التعديل أو التحديث على مستوى حماية وأمان البيانات الشخصية.

الفصل الثامن

الجزاءات والمخالفات

المادة (146): مخالفة شروط صحة التوقيع الإلكتروني

دون الإخلال بالجزاءات المنصوص عليها في التشريعات النافذة، يُعد استخدام أي توقيع إلكتروني غير صادر عن وسيلة معتمدة أو مخالف للضوابط الفنية سببًا للمساءلة، ويترتب عليه:

1. إلغاء التوقيع الإلكتروني.
2. بطلان المحرر الإلكتروني المرتبط به.

المادة (147): الإخلال بحماية بيانات إنشاء التوقيع

على الهيئة تعليق الشهادة الرقمية إذا لم يتخذ صاحب التوقيع الإجراءات اللازمة لحماية مفتاحه الخاص، أو لم يُبلّغ فورًا عن فقدانه أو اختراقه، وعند تكرار المخالفة يُحال إلى إلغاء الشهادة نهائيًا.

المادة (148): تعديل المحررات الإلكترونية بعد التوقيع

تعديل المحرر الإلكتروني بعد توقيعه دون إعادة توقيع النسخة المعدلة أو توثيق التعديل تقنياً وفق أحكام اللائحة، يُعد سببًا لفقدان المحرر قيمته القانونية.

المادة (149): فقدان شروط الحفظ الإلكتروني

عدم الالتزام بوسائط الحفظ المعتمدة أو فقدان خصائص المحرر الأصلية يؤدي إلى عدم تمتع المحرر بالحجية القانونية المقررة للمحررات الإلكترونية.

المادة (150): مزاولة نشاط التصديق الإلكتروني دون ترخيص

يُعد كل شخص طبيعي أو اعتباري يزاول نشاط تقديم خدمات التصديق الإلكتروني دون ترخيص ساري مخالفًا للائحة، ويترتب عليه:

1. إصدار تعميم فوري بمنعه من النشاط.
2. إدراجه في قائمة الممنوعين من التقدم للحصول على ترخيص.
3. إخطار الجهات المختصة والنيابة العامة بذلك.

المادة (151): إصدار شهادات دون تحقق أو ببيانات غير صحيحة

عند ثبوت إصدار شهادة مصادقة إلكترونية دون التحقق من هوية طالب الشهادة أو ببيانات غير صحيحة، تُبطل الشهادة، ويُتخذ ما يلزم لمساءلة مقدم الخدمة، بما في ذلك المساءلة التأديبية.

المادة (152): عدم تحديث الشهادات الملغاة أو المعلقة

عدم تحديث مزود الخدمة لقائمة الشهادات الملغاة أو المعلقة خلال المدة المقررة، يُعد مخالفة، ويترتب عليه:

1. تعليق ترخيص مقدم الخدمة لمدة لا تقل عن 3 أشهر ولا تزيد على سنة.

المادة (153): الاحتفاظ بعناصر إنشاء التوقيع الخاصة بالمستخدمين

يُحظر على مقدم الخدمة الاحتفاظ بنسخة من المفتاح الخاص للمستخدم، ويُعد ذلك سببًا لسحب الترخيص نهائيًا.

المادة (154): الإخلال بإجراءات الإخطار في حالات التعليق أو الإلغاء

عدم إخطار المستفيد بقرار تعليق أو إلغاء الشهادة خلال 24 ساعة، يؤدي إلى بطلان الإجراء.

المادة (155): مخالفة التزامات الإفصاح في التجارة الإلكترونية

عدم الالتزام بتقديم البيانات الواجبة للمستهلك وفق أحكام اللائحة يُعد مخالفة، ويترتب عليه:

1. بطلان العقد أو الشروط المخالفة.
2. حق المستهلك في التعويض عن الأضرار الناتجة.

المادة (156): التأخر في تسليم المنتجات أو الخدمات

عدم تسليم المنتج أو الخدمة خلال المدة المحددة دون إخطار مسبق يؤدي إلى فسخ العقد تلقائيًا، واسترجاع المبلغ كاملاً.

المادة (157): عدم توفير آلية إلغاء إلكترونية

عدم توفير أيقونة "إلغاء عقدك" أو وسيلة إلكترونية لإتمام الإلغاء، يعد الإلغاء نافذًا، ويلزم البائع بجميع الآثار القانونية والتعويض عند الاقتضاء.

المادة (158): مخالفة المصارف لمعايير الأمن السيبراني

عدم التزام المصارف أو المؤسسات المالية بمعايير الأمن السيبراني أو عدم الإبلاغ عن الحوادث، يُعد مخالفة، ويترتب عليه:

1. مسؤولية عن تعويض المتضررين.
2. إدراج المخالف في التقرير الفصلي للهيئة.
3. حق الهيئة في تجميد خدمات إلكترونية محددة.

المادة (159): فرض رسوم غير معلن عنها

فرض أي رسم أو عمولة غير منصوص عليها في العقد أو غير معلن عنها يُعد مخالفة، ويترتب عليه:

1. بطلان الرسوم.
2. إلزام المؤسسة بإعادة المبالغ للعميل.

المادة (160): فرض رسوم غير معلن عنها

جمع أو معالجة أو الاحتفاظ بالبيانات الشخصية دون موافقة صريحة أو سند قانوني يُعد مخالفة، ويترتب عليه:

1. اعتبار المعالجة غير قانونية.
2. مسؤولية الجهة عن أي أضرار.

المادة (161): عدم تمكين صاحب البيانات من حقوقه

عدم تمكين صاحب البيانات من الاطلاع أو التعديل أو الحذف يُعد مخالفة، ويترتب عليه:

1. تصحيح الوضع فورًا.
2. إنذار رسمي.
3. تعليق الترخيص عند تكرار المخالفة.

المادة (162): تشغيل مو اقع إلكترونية دون ترخيص

إنشاء أو تشغيل مواقع إلكترونية دون ترخيص من الهيئة أو دون الالتزام بالضوابط والمعايير، يُعد مخالفة، ويترتب عليه:

1. وقف الموقع فورًا.
2. مساءلة الممثل القانوني للمؤسسة.

الفصل التاسع
الأحكام العامة والختامية

المادة (163):

يمنح بقرار من مجلس الوزراء بناء على عرض من الهيئة صفة مأمور الضبط القضائي في مجال المعاملات إلكترونية لموظفي الهيئة على أن تتوفر الشروط الآتية:

1- أن يكون ليبي الجنسية.

2- أن تكون لديه الخبرة في مجال تخصصه.

3- أن يكون لديه مؤهل علمي في المجالات ذات العلاقة بالآمن السيبراني (القانون والمعلوماتية).

المادة (164):

تعتبر جميع المعايير والسياسات والتعليمات والاستراتيجية والقرارات الصادرة عن الهيئة ملزمة لجميع الوزارات والقطاعات والدوائر الحكومية والجهات التابعة لها، بما في ذلك مؤسسات القطاع الخاص في إطار الأمن السيبراني.

المادة (165):

تلتـزم كافـة المؤسسـات العامـة والخاصـة بـإبلاغ الهيئـة عمـا تتعـرض لـه مـن حـوادث أو تهديدات سيبرانية حسب الضوابط التي تضعها الهيئة.

المادة (166):

علـى جميـع الخاضـعين لهـذه اللائحـة تسـوية أوضـاعهم بمـا يتفـق مـع أحكامهـا فـي أجل أقصاه ستة أشهر من دخولها حيز النفاذ.

المادة (167):

يُعمل بهذه اللائحة اعتباراً من تاريخ صدورها وتنشر بالجريدة الرسمية.