地域	*リビア*
日付	*2022 年 9 月 18 日*
法律事務所	*Zahaf & Partners Law Firm*
役職名、氏名	*Dr. Saleh Zahaf – Partner* *Mahmud Zahaf - Partner*
連絡先	*Tel: 00218 21 3334636 | 00218 21 3345761 | Fax: 00218 21 3343515* *Email: mahmud.zahaf@zahaflaw.com* *Email: Saleh@zahaflaw.com*

質問事項

I. 個人情報保護に関する法律

i. あなたの国には、現在または近い将来の予定として**民間分野**における個人情報保護に関する一般法はありますか。

包括的な法令はありません。リビア議会は 2021 年に電子取引法を制定しましたが、この法律は公表されていないか、一般に公開されていません。この法律の規定は今日まで不明のままです。

ii. あなたの国には、現在または近い将来の予定として**公的分野**における個人情報保護に関する一般法はありますか。

国家情報セキュリティおよび安全ポリシー

iii. あなたの国には、現在または近い将来の予定として**個別の（特定の）分野に適用のある**個人情報保護に関する法律はありますか。（ある場合は概要をご教示ください。）

リビアには、個々の(特定の)分野に適用される個人情報の保護に特に対処する法律はありません。

I の(i)(ii)(iii)について全て「該当なし」の場合は IV に進みます。

II. 個人情報保護に関する規制の基本情報

i. I で言及いただいた個人情報保護に関する法律について以下の空欄を埋めて下さい。

名称：*国家情報セキュリティおよび安全ポリシー*

① 「個人情報」の定義	*「個人情報」は定義されていませんが、社会保障番号や国民 ID 番号、パスポート番号、クレジットカード番号、運転免許証番号、医療記録などの個人を特定できる情報と*

	して説明されています。
② 法の適用範囲	*このポリシーは、すべての省庁、公共部門、政府部門、およびそれらの関連機関の業務に対する拘束力を有します。*
③ 地理的範囲	*このポリシーは、ローカルおよびグローバル規模で適用されます。*
④ URL	*https://nissa.gov.ly/wp-content/uploads/NISSA_Policy_Manual_v1.0-1.pdf*
⑤ **施行**日	*不明です。*

ii. 上記の法について特に言及すべき事項がございましたらその概要をご教示下さい。

III. OECD プライバシー原則

i. OECD プライバシーガイドラインの各原則を具体化した法の条文があればご教示下さい。
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) 収集制限の原則

この原則は、個人データの収集には制限を設け、いかなる個人データも、適法かつ公正な手段によって、及び必要に応じてデータ主体に通知し、又は同意を得た上で収集すべきであることを意味します。

該当なし

(b) データ内容の原則

この原則は、個人データは、利用目的の範囲内において利用し、かつ利用目的の達成に必要な範囲内で正確、完全及び最新の内容に保つべきであることを意味します。

該当なし

(c) 目的明確化の原則

この原則は、個人データの収集目的は、データが収集された時点よりも前に特定し、当該利用目的の達成に必要な範囲内における事後的な利用又はその他の目的での利用は、その利用目的に矛盾しない方法で行い、利用目的を変更するにあたっては毎回その利用目的を特定すべきであることを意味します。

該当なし

(d) 利用制限の原則

この原則は、個人データは、以下の場合を除き、(c)目的明確化の原則により特定された目的以外の目的のために開示すること、利用可能な状態に置くこと又はその他の方法で利用すべきではないことを意味します。

i) データ主体の同意がある場合

ii) 法令に基づく場合

国家情報セキュリティおよび安全ポリシーに部分的に規定されています。
-データ保護ポリシーのセクション2「情報保護ポリシー」パラグラフ2.4.3「情報開示」。
-データ保護ポリシーのセクション4「情報拡散ポリシー」。
-データ保護ポリシーのセクション5「情報ポリシーへのアクセス」。
これらの規定に基づき、本ポリシーは、個人情報の共有を経営陣から許可を得た者に対する共有のみに制限しています。さらに、このポリシーの下で、個人情報が共有/開示される場合、文書化された情報共有プロトコルまたはデータ交換契約に従ってのみ行う必要があります。

(e) 安全保護の原則

この原則は、個人データは、その滅失若しくは不正アクセス、毀損、不正利用、改ざん又は漏えい等のリスクに対し、合理的な安全保護措置を講ずるべきであることを意味します。

国家情報セキュリティおよび安全ポリシーのネットワークセキュリティポリシーに規定されています。
このポリシーは、取得した個人情報を保護するために適用する必要のある手順と保護を公的機関に指示しています。

(f) 公開の原則

この原則は、個人データの活用、取扱い、及びその方針については、公開された一般的な方針に基づくべきであり、その方法は、個人データの存在及び性質に応じて、その主要な利用目的とともにデータ管理者の識別及び通常の所在地を認識できる方法によって示すべきであることを意味します。

該当なし

(g) 個人参加の原則

この原則は、個人が次の権利を有することを意味します。

i) データ管理者が自己に関するデータを保有しているか否かについて、データ管理者又はその他の者から確認を得ること。

ii) 自己に関するデータを保有している者に対し、当該データを、
合理的な期間内に、
必要がある場合は、過度にならない費用で、
合理的な方法で、かつ、
本人が認識しやすい方法で自己に知らしめられること。

iii) 上記 i）及び ii）の要求が拒否された場合には、その理由が説明されること及びそのような拒否に対して異議を申し立てることができること。

iv) 自己に関するデータに対して異議を申し立てること及びその異議が認められた場合には、そのデータを消去、訂正、完全化、改めさせること。

該当なし

(h) 責任の原則

この原則は、データ管理者が、上記の諸原則を実施するための措置を遵守する責任を有することを意味します。

該当なし

ii. OECD プライバシーガイドラインの各原則が適用されない分野があればその概要をご教示下さい。

(a) 収集制限の原則

(b) データ内容の原則

(c) 目的明確化の原則

(d) 利用制限の原則

(e) 安全保護措置の原則

(f) 公開の原則

(g) 個人参加の原則

(h) 責任の原則

Ⅳ. ガバメントアクセスとデータローカライゼーション

あなたの国において、包括的ガバメントアクセス（例：捜査目的で当局が個人データにアクセスする際の制限）やデータローカライゼーション（例：サーバやデータの国内設置及び保管を義務付ける規制）のような、個人データの主体の権利に影響を及ぼすような仕組みはございますか。ある場合は、その内容をご教示下さい。

データローカライゼーションのための仕組みはありませんが、ガバメントアクセスのための規制として、次のものがあります。

・リビア銀行法（2005 年法律第 1 号） 第 116 条

本法律および本法律に基づき発行された規則・政令の規定に違反して発生した犯罪に関して、調査官として指名されたリビア中央銀行の職員は、記録、引落口座、その他の文書・記録、および電子システムを調査することができます。

https://www.almontaser.com/Laws/Law%20No.%20(1)%202005%20regarding%20banks.pdf

・マネー・ローンダリング防止に関する法律（2005 年法律第 2 号） 第 14 条

この法律の規定に従い、情報またはデータを入手したすべての主体は、その機密を保持し、マネー・ローンダリング犯罪およびその他の犯罪に関する捜査、起訴および事件で使用するために必要な場合を除き、それらを開示してはなりません。

https://security-legislation.ly/en/law/31549

・リビア刑法 第 469 条

正当な理由なく、騒乱その他の災害または現行犯が発生した場合に、公務員がその職務を行うにつき援助を提供せず、もしくはその求めに応じず、または前記の場合に必要な情報やデータを提供しなかった者は、1 か月以下の拘留または罰金に処せられます。

https://security-legislation.ly/sites/default/files/lois/290-Penal%20Code_EN.pdf

・コミュニケーション法（2020 年法律第 22 号） 第 15 条

通信サービスを提供する事業者は、受益者の通信の機密性を確保するためにあらゆる措置を講じなければならず、サービスの受益者の通信を傍受、監視、変更または修正してはなりません。

嫌がらせ、攻撃的または違法な電話に対するフォローアップ、所在確認または対応のため、

または法律で認められる場合：

a. 受益者は、サービス提供者に自分の電話に関連する通話を監視するように要求することができます。

b. 法的権限のある司法当局は、サービスを提供する事業者に対して、個人の電話への着信または発信の通話を傍受または監視するよう指示を出すことができ、その事業者は、それらの指示に従わなければなりません。

サービス提供者は、通話に用いられた電話番号やその日付など、個人の電話の監視から得られた情報を当該機関に提供しなければなりません。

c. 所管官庁は、嫌がらせ、敵対的または違法な電話から人々を保護するための措置を講じ、また所管官庁に照会して必要な措置を講じさせることができます。

https://security-legislation.ly/en/law/34009#:~:text=No%20telecommunications%20networks%20may%20be,and%20the%20implementing%20regulations%20thereof

・サイバー犯罪防止法（2022 年法律第 5 号）

第 7 条

国家安全保障情報安全局は、国際情報ネットワークまたはその他の技術システムを通じて公表および表示されるものを監視し、社会の安全と安定を損ない、または社会の平和を害する偏見や思想を広めるものをすべて阻止することができます。電子メールまたは会話は、管轄地方裁判官が発する司法命令による場合を除き、監視することはできません。

第18条

情報システムで使用される他人の識別子および識別手段を違法に入手した者は、禁固刑および 1,000 ディナール以上 3,000 ディナール以下の罰金に処されます。

故意に、かつ違法に、情報システムにおいて他人に属する識別子および識別手段を使用した者は、1 年以上の禁固刑および 1,000 ディナール以上 1 万ディナール以下の罰金に処されます。

https://lawsociety.ly/legislation/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-5-%D9%84%D8%B3%D9%86%D8%A9-2022-%D9%85-%D8%A8%D8%B4%D8%A3%D9%86-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7/

V. データ保護機関

データ保護機関がある場合は、名称と住所をご教示下さい。

名前: The National Information Security & Safety Authority
住所:V5FR + 33W、シャリアアルジャラア、トリポリ
電話: +218 21 361 41 15
ホームページ: https://nissa.gov.ly/
その他の情報: