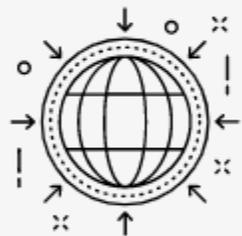


令和2年改正個人情報保護法への対応の振り返り ～楽天グループ株式会社～

辻畑 泰喬 (Tsujiyata, Yasutaka)
グローバル・プライバシー・オフィス (GPO)
楽天グループ株式会社



世界に喜びと楽しさを。
楽天は世界中の人々に、革新的な
インターネットサービスとフィンテックサービスをお届けします。



サービス展開拠点

30 カ国・地域



グループサービス
利用者数

16 億



サービス数

70 超



グローバル流通総額

26.9 兆円

*2021年度

サービス事業



コマースカンパニー >



アド & マーケティングカンパニー >



コミュニケーションズ & エナジーカンパニー >

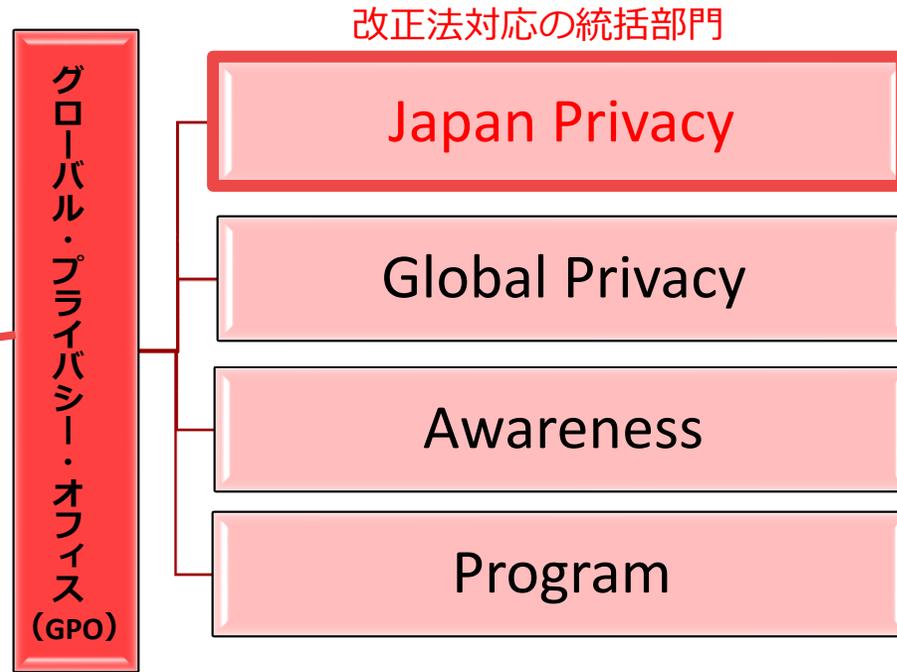
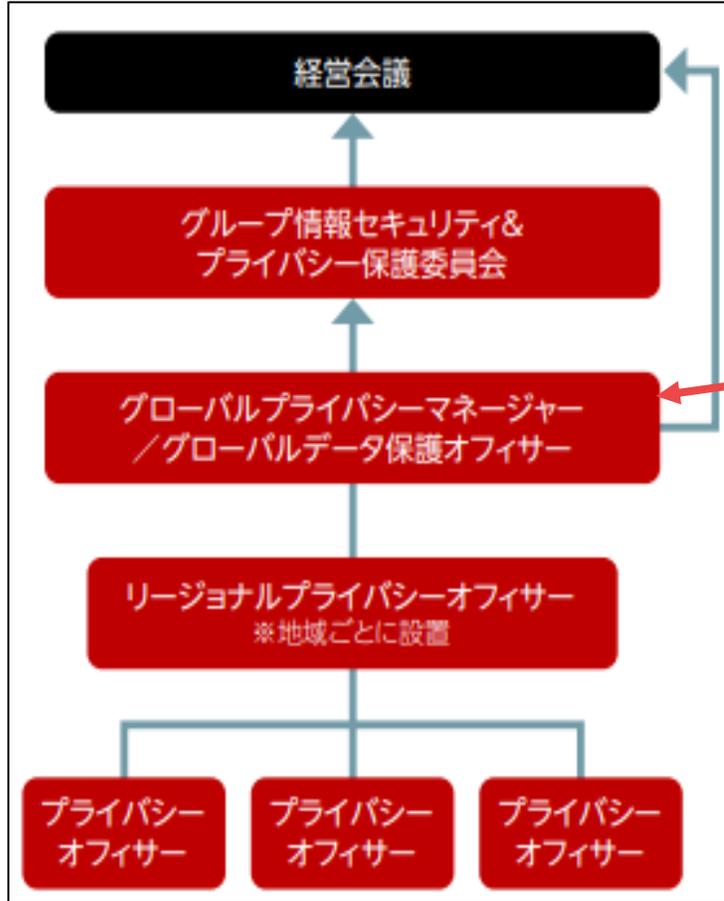


インベストメント & インキュベーションカンパニー >



フィンテックグループカンパニー >

グローバル・プライバシー・オフィス (GPO)

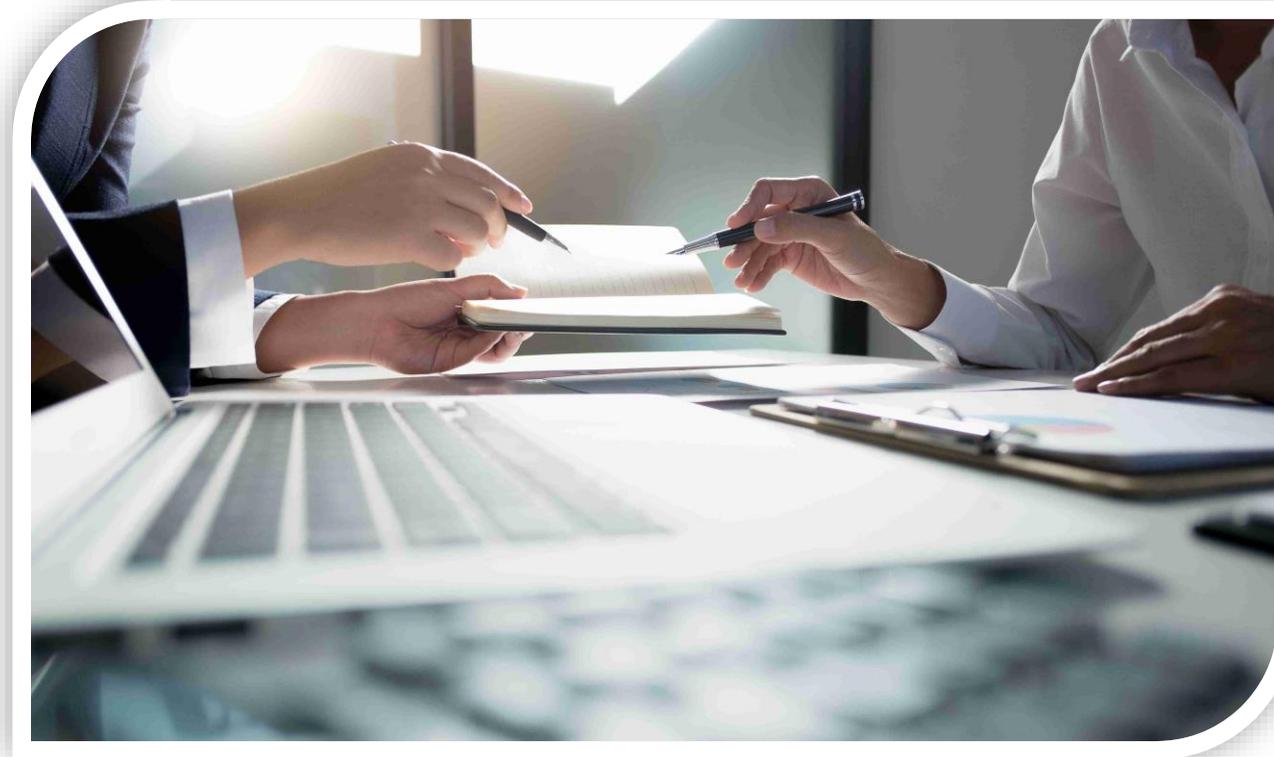


コンサルティングファーム



コンサルティングファーム

- 短期的にマンパワーが必要
 - 関係各所とのミーティングや連絡
 - ドキュメンテーション
 - イントラサイトページの作成
 - プロジェクトの推進者
 - その他各種相談
- 平常業務との両立
- 内部者として案件に迅速かつ柔軟に対応
- 法律業務ではなくロジ的な作業
- 法改正やプライバシー関連業務の知見
- ノウハウ



改正法の施行

外国における制度等の調査
結果の公表

ガイドラインの改正等

政令・規則の改正

改正法に関連する政令規則
等の整備に向けた論点

令和2年改正個人情報保
護法の成立

個人情報保護法
いわゆる3年ごと見直し
制度改正大綱



2019年
12月

2020年
6月

10月～11月

2021年
3月

8月

2022年
1月

4月

楽天グループ株式会社

Kickoff MTG
(全体)

Kickoff MTG
(個別)

①情報収集・社内周知

②改正法プロジェクトの本格始動

③対象事業の特定

④対象事業へのインプリ

情報収集

- 法令、ガイドライン、QA、パブコメ、その他の個人情報保護委員会公表資料（◎）
- 個人情報保護委員会セミナー（◎）
- 事業者団体等のセミナー（◎ or ○）
- 法律事務所セミナー（○）
- 書籍、法律雑誌（○）
- 他事業者や個人情報保護委員会との意見交換会（○）
- ウェブサイトの記事（△）
- 有料セミナー（× 利用せず）

社内周知

- 説明会等
 - ▶ 全体事前説明会（複数回）
 - ▶ 部門内（テクノロジー部門等）
 - ▶ CCO会議
 - ▶ 全体キックオフ
 - ▶ 個別キックオフ（カンパニー、事業）
 - ▶ 経営会議（月例）
- レクチャー動画
- 個別ミーティング
- イントラ
- ニュースレター
- ポスター

対象事業の特定

各組織への簡易質問票の送付

×2

※多数の部署

※用語説明のリンク

※できる限り簡易な質問

簡易質問票等のレビュー

※ISMS台帳

※これまでの知見

レビュー結果を踏まえた個別
ミーティング

→ **対象事業の特定**

※インプリ段階でスコープインすることも

簡易質問票（例）

APPI - Screening

表示

はじめに

Basic Questions（基本情報） >

Additional Questions（追加情報） >

1.3 *あなたの部署では、パーソナルデータを第三者から受領していますか？ /
Does your organization receive personal data from a third party?

パーソナルデータ、第三者、受領の定義に関しましては、下記リンクをご参照ください。

For the definition of personal data, third party and reception of data, please refer to the link below.

<https://confluence.rakuten-it.com/confluence/x/2uitpQ>

No Yes

0 0

1.4 *あなたの部署では、パーソナルデータを第三者に提供していますか？ /
Does your organization provide personal data to a third party?

パーソナルデータ、第三者、提供の定義に関しましては、下記リンクをご参照ください。

For the definition of personal data, third party and provision of data, please refer to the link below.

<https://confluence.rakuten-it.com/confluence/x/2uitpQ>

キックオフミーティング（全体&対象事業）

＜対象事業とのキックオフミーティングの場合＞

- 基本的に個々の対象事業単位（ただし、統合して実施の場合も）
- 30分～1時間程度（事業によっては以後複数回のミーティング）
（趣旨）
- GPO担当者と対象事業との顔合わせ
- 対象事業のPICの設定
- 本プロジェクト及び法改正の概要説明
- 期限等のスケジュール及び進捗報告方法の確認
- 簡易質問票等の内容確認
- 個別論点に関連する事実の大まかな確認
- コミュニケーション方法の確認
- 今後の進め方の確認 等



対象事業とのコミュニケーション方法

- 社内イントラに改正APPI専用の情報共有ページを作成
 - ①改正法の概要資料
 - ②各改正項目への対応事項及び全体スケジュール
 - ③各サービスにおけるタスクの詳細
 - ④各改正項目についてのガイドライン等
 - ⑤過去の説明会動画等の一覧
 - ⑥その他の共有事項
 - ⑦質問コーナー 等
- メーリングリスト
- 専用のGPOメールアドレス
- FAQ
- タスク管理ツール

※社内イントラの専用ページの一部抜粋

各改正項目についてのガイドライン等	
各改正項目にかかるガイドラインはこちらです。	
改正項目	ガイドライン
1外国への個人情報の提供に関する説明事項の充実（第三者提供）	個人データの越境移転ガイドライン
2外国への個人情報の提供に関する説明事項の充実（委託）	
3利用停止・消去の義務の強化	利用停止・消去の対応ガイドライン
4第三者提供記録の開示	第三者提供記録ガイドライン
5個人関連情報を収集し個人データと紐づけて利用するときの同意取得	個人関連情報ガイドライン
その他の資料はこちらです。	
テーマ	

タスク管理ツール

Issues in Epic

✓ GPOA-4150	[Redacted]	↑	CLOSED
✓ GPOA-4151	[Redacted]	↑	CLOSED
✓ GPOA-4152	[Redacted]	↑	CLOSED
✓ GPOA-4153	[Redacted]	↑	CLOSED
✓ GPOA-4154	[Redacted]	↑	CLOSED
✓ GPOA-4155	[Redacted]	↑	CLOSED
✓ GPOA-4156	[Redacted]	↑	CLOSED
✓ GPOA-4157	[Redacted]	↑	CLOSED
✓ GPOA-4158	[Redacted]	↑	CLOSED
✓ GPOA-4159	[Redacted]	↑	CLOSED
✓ GPOA-4160	[Redacted]	↑	CLOSED
✓ GPOA-4161	[Redacted]	↑	CLOSED
✓ GPOA-4162	[Redacted]	↑	CLOSED
✓ GPOA-4163	[Redacted]	↑	CLOSED

Global Privacy Office - Audit / GPOA-2850
(Investigation) 第三者提供先リストの作成 Create a list of companies/vendors to whom overseas third-party provision of d

Edit Comment Assign More Put on Hold For Approval Back to Resolve

Details

Type: Improvement Status: CLOSED (View Workflow)
Component/s: Implementation - Milestone Resolution: Fixed
Labels: APP1_M02 APP1_R1.2 APP1_R2.2 APP1_R4.1
Business Unit: [Redacted]
Product Area: [Redacted]
Category: [Redacted]
Project ID: [Redacted]
Epic Link: [Redacted]

People

Assignee: [Redacted]
Reporter: CC (Individual user): [Redacted]
Votes: [Redacted]
Watchers: [Redacted]

Description

進捗管理

Virtual Company

Select

Service

Filter by...

Reporter

Legal Req.

Select all (9)

1 2 3 4 5 6 7 8 9



63 Tickets in current selection

Service	Legal Req	Summary	Due Date	Last Updated	User Last Updated	Task Status	Issue Key
	2.1		2021-10-31	2022-01-12 07:44:50		COMPLETED	GPOA-5004
	2.2		2022-01-14	2022-02-27 06:39:48		COMPLETED	GPOA-5005
	2.3		2022-03-31	2022-01-24 10:16:17		SCOPE OUT	GPOA-5023
	2.1		2021-10-31	2022-01-12 06:59:20		COMPLETED	GPOA-2667
	2.2		2022-01-14	2022-03-09 00:15:37		COMPLETED	GPOA-2668
	2.3		2022-03-31	2022-01-24 08:33:30		SCOPE OUT	GPOA-2686
	2.1		2021-10-31	2021-12-05 07:17:34		COMPLETED	GPOA-2849
	2.2		2021-12-29	2022-03-20 01:23:19		COMPLETED	GPOA-2850
	2.3		2022-03-31	2022-03-20 01:23:42		SCOPE OUT	GPOA-2868
	2.1		2021-10-31	2022-01-12 08:13:13		COMPLETED	GPOA-2928

<フィルター>

<一覧表>



等

フィルターごとの状況を一覧で確認可能

法的対応事項のイメージ（初期＜ガイドライン公表前＞のもの）

※令和2年改正への企業における法的対応事項概要（規程や覚書などの記載は絶対的なものではなく、一つの対応例）

改正事項	改正/新設	データマッピング	適用関係調査	【インプリ】				
				適用の際の対応	プラボリ/規約への直接的影響	社内規程等の改定	覚書等の改定	社内周知
1 不適正な利用の禁止 (法16条の2)	新設							
2 漏えい等の報告 (法22条の2)	新設（告示からの格上げ）							
3 外国の第三者への提供に係る情報提供・確認（法24条）	改正							
4 個人関連情報の提供に係る同意取得・確認（法26条の2）	新設							
5 開示方法の選択及び開示対象の拡大（法28条）	改正							
利用停止、消去、第三者								



主な検討事項

1

外国提供（第三者、委託）

2

第三者提供時の確認・記録の再確認

3

利用停止等

4

個人関連情報

5

プライバシーポリシー等による説明

- ・外国の名称や制度等
- ・利用目的の具体化
- ・安全管理措置
- ・事業者に関する情報
- ・個人情報等の突合 等

外国提供（制度調査）

- 主にトラベル系事業
- 個人情報保護委員会の制度調査と楽天における追加調査
- 分野別法令により制度調査内容は異なり得る
- 特殊分野の制度調査が必要になった場合
- 多数の国の調査
- 継続的なアップデート
- 説明事項の長文化

ウズベキスタン共和国															
I. サマリー															
個人情報の保護に関する制度の有無	包括的な法令として、以下の法令が存在する。 ■ 個人データ法 (Law of the Republic of Uzbekistan No. ZRU-547 "On Personal Data") - URL : https://lex.uz/docs/4831939 - 施行状況 : 2019年10月1日施行 - 対象機関 : 公的部門及び民間部門 - 対象情報 : 電子媒体、紙媒体その他の有形の媒体に記録された特定の個人に関する情報又は特定の個人を識別できる可能性につながる情報														
個人情報の保護に関する制度についての指標となり得る情報	EUの十分性認定 : なし APECのCBPRシステム : なし														
OECD プライバシーガイドライン8原則に対応する事業者の義務又は本人の権利	OECD プライバシーガイドライン 8 原則に対応する事業者の義務又は本人の権利については、以下のとおり。 <table border="1"><tbody><tr><td>① 収集制限の原則</td><td>上記法令に一部規定されている。</td></tr><tr><td>② データ内容の原則</td><td>上記法令に規定されている。</td></tr><tr><td>③ 目的明確化の原則</td><td>上記法令に規定されている。</td></tr><tr><td>④ 利用制限の原則</td><td>上記法令に規定されている。</td></tr><tr><td>⑤ 安全保護の原則</td><td>上記法令に規定されている。</td></tr><tr><td>⑥ 公開の原則</td><td>上記法令に該当する規定は不相当である。</td></tr><tr><td>⑦ 個人参加の原則</td><td>上記法令に規定されている。</td></tr></tbody></table>	① 収集制限の原則	上記法令に一部規定されている。	② データ内容の原則	上記法令に規定されている。	③ 目的明確化の原則	上記法令に規定されている。	④ 利用制限の原則	上記法令に規定されている。	⑤ 安全保護の原則	上記法令に規定されている。	⑥ 公開の原則	上記法令に該当する規定は不相当である。	⑦ 個人参加の原則	上記法令に規定されている。
① 収集制限の原則	上記法令に一部規定されている。														
② データ内容の原則	上記法令に規定されている。														
③ 目的明確化の原則	上記法令に規定されている。														
④ 利用制限の原則	上記法令に規定されている。														
⑤ 安全保護の原則	上記法令に規定されている。														
⑥ 公開の原則	上記法令に該当する規定は不相当である。														
⑦ 個人参加の原則	上記法令に規定されている。														

国外における個人情報の保護のための制度等に関する情報提供

個人情報の提供先となり得る日本国外の国における個人情報の保護に関する制度等については、以下の個人情報保護委員会のウェブサイトをご参照ください。

外国における個人情報の保護に関する制度等の調査

上記ウェブサイトに記載のない国につきましては、以下をご参照ください。

- > ウズベキスタン共和国
- > エジプト
- > エチオピア
- > 北マリアナ諸島自治連邦区
- > スリランカ
- > セーシェル
- > タヒチ

- > チリ
- > ニューカレドニア
- > パプアニューギニア
- > パラオ共和国
- > フィジー共和国
- > ブルネイ
- > マカオ

< 随時追加予定 >

なお、個人情報の提供先となる国において「OECDプライバシーガイドライン」の8原則に対応する措置を講じていない場合であっても、提供先との契約において当該措置を講じることを義務づけた上で個人情報の提供を行っています。

外国提供（基準適合体制の整備）

- DPA（Data Processing Addendum）のアップデートと締結
- 利用規約でのサービス利用の可否
- DPAの締結交渉
楽天ひな型 or ベンダーひな型
- 法第4章第2節の規定の趣旨
- DPAの文言交渉
- そもそもAPPI（個人情報保護法）がDPAの適用対象外のケース
- 適用法令を遵守の条項もないケース
- DPAの締結事実のみで満足しない
- ベンダー主張のDPAを締結せざるを得ない力関係
- APPIのプレゼンス

Data Processing Addendum[↵]

↵

THIS ADDENDUM is made on [DD MMMM YYYY] ("Effective Date")[↵]

BETWEEN:[↵]

(1) [Controller full name] a company incorporated in [Country] with its place of business at [Address] ("Controller"); and[↵]

(2) [Processor full name], a company incorporated in [Country] with its place of business at [Address] ("Processor")[↵]

together the "Parties" and each a "Party",[↵]

↵



開示等請求

- 各事業が管理している個人情報の在処とその内容
- 各事業管理、共通管理
- 対応が想定される場面の確認
- 削除や利用停止の具体的アクション
- システム改修の要否
- 担当者間の連携方法**
- 社内プロセスの再確認と書面による明確化**

※イメージ

開示等請求対応プロセス↓
<会社名/部署名>←

←

•1. 目的←
開示等請求対応プロセス（以下、「本プロセス」といいます）は、上記会社または部署（以下「本組織」と……………←
←
……………←
←

•6. 本プロセス←

•6.1 本組織における開示等請求のプロセス←
6.1によりGPOから開示等に関する作業依頼を受けた場合、作業が必要となるシステム、作業担当者、必要となるアクションは……………←
←

# ←	Where: ← システムや ツール ←	Who: ← 作業担当者または 担当部署 ←	What: ← アクション ←
1 ←	←	←	開示: ← 消去等: ←
2 ←	←	←	開示: ↓ 消去等: ←
3 ←	←	←	開示: ←

プライバシーポリシー

- 30以上のプライバシーポリシーをアップデート
 - ①事業者に関する情報
 - ②利用目的の説明
 - ③外国提供
 - ④突合による広告配信等
 - ⑤個人関連情報
 - ⑥安全管理措置 等
- ログイン時等の同意取得
- 文書の長文化、難解化
- プライバシーポリシーの位置づけをどうすべきか
- 説明だけしておけばよいという発想からの脱却

楽天グループ株式会社「個人情報保護方針」の改定について

楽天グループ株式会社は、2022年4月1日施行の改正個人情報保護法が事業者に求めている事項に対応するため、2022年3月31日付で「個人情報保護方針」の一部を改定することとなりました。

■2022年3月31日改定 個人情報保護方針

このたびの改定では、以下の点について説明事項の追加を行っております。

1. 事業者に関する情報
2. 利用目的のより詳細な特定
3. 国外への個人情報の移転について
4. 個人情報の突合による広告配信等について
5. 個人関連情報を個人データとして取得することについて
6. 安全管理措置について

それぞれの説明事項について、目的と概要をご説明いたします。

1. 事業者に関する情報

「個人情報保護方針」が適用される楽天グループの各社について、従来から会社名をお示ししておりましたが、これに「会社概要」へのリンクを追加し、各社の住所および代表者氏名をご確認いただけるようになりました。

> 該当箇所：「1. はじめに」ほか

2. 利用目的のより詳細な特定

お客様の個人情報の利用についてより透明性を高めるべく、以下の点について説明を追加いたしました。

- ・ 広告宣伝やサービスの改善のため、AI等を用いてお客様の購買傾向を分析・利用する場合があります
- ・ お客様によるサービスの利用終了後に、お問い合わせ対応やアフターサービス等のために個人情報を利用する場合があります

最終改定日：2022年3月31日
改定前の方針はこちら

個人情報保護方針

1. はじめに	2. 取得する個人情報	3. 個人情報の利用、利用の法的根拠、保持
4. お客様の個人情報にアクセスする旨	5. お客様に関連する情報の取得	6. お客様の権利とお客様による選択
7. 個人情報の確認等	8. セキュリティおよび国外への移転	9. 本方針の変更

楽天グループ株式会社（以下「楽天」といいます。）並びにその子会社および関連会社で構成される楽天グループ（以下単に「楽天グループ」といいます。）は、多種多様なサービスを提供しています。お客様によるサービスのご利用に際して、楽天グループは、お客様の情報を取得および利用し、また、当該情報を保管しています。

楽天グループ株式会社が定めるこの個人情報保護方針（以下「本方針」といいます。）は、本方針を採用する楽天グループの会社がお客様の個人情報を取得して取扱う目的および方法を明らかにし、個人情報に関するお客様の権利について理解を深めていただくためのものです。楽天グループは、お客様によるサービスのご利用にあたり、ご自身の情報がどのように取扱われるか、十分にご理解いただけるよう取り組んでいます。

「お客様の個人情報の利用について」もあわせてご覧ください。

1. はじめに

本方針は、楽天または本方針を採用する楽天グループの会社（以下「私たち」*といっています。）が提供するサービス（関連する付帯サービス、アプリケーション、ツール等を含み、以下「対象サービス」といいます。）をお客様がご利用になる場合に適用されます。なお、私たちおよびその他の楽天グループの会社は、サービスの内容等に応じて、本方針に付加して、または本方針とは別に、個人情報の取扱い

プライバシーセンター

・ プライバシーセンターにコンテンツを追加

- ① プライバシーってなんだろう？
- ② Rakuten IDってなんだろう？
- ③ 個人情報保護方針ってなんだろう？
- ④ Cookieってなんだろう？

個人情報保護方針ってなんだろう？

これまでに「個人情報保護方針」や「プライバシーポリシー」という用語を聞いたことがありませんか？それらは一体どのようなもので、どう理解すればいいのでしょうか？今回はそのような疑問についてお答えしたいと思います。



企業が個人に関する情報を収集して使用する時、多くの国（日本、EU、アメリカなど）では企業がどのようにその情報を集めるか、なぜ集めるのか、どのように利用するのかなどを利用者に説明しなければなりません。

これは通常、「個人情報保護方針」もしくは「プライバシーポリシー」といったタイトルのページで説明されており、企業のWebサイトの最下部に表示されているリンク先から閲覧できるなど、簡単にアクセスできるようにデザインされています。

個人情報保護方針では、いくつかの重要な事項が説明されていますが、契約書などのように、内容が難しいことが多いため、きちんと理解するのに時間がかかるかもしれません。ここでは、個人情報保護方針で最も重要な情報を効率的に見つける方法を説明します。

多くの個人情報保護方針はいくつかの章に分かれています。企業によってタイトルや構成は様々ですが、以下のような内容が説明されています。

- (1) 誰があなたのデータを収集するのか？
- (2) どのようなデータが収集されるのか？
- (3) なぜ収集されるのか？
- (4) 誰と共有されるのか？
- (5) あなたの権利は何か？

まず、誰があなたのデータを収集しているのかを最初に確認できるようになっています。想定していた企業名でしたか？もしくは違う企業名でしょうか？個人情報保護方針に運営会社名が記載されていなかったり、サービス名なのか会社名なのか分からない名称になっていたりと、「誰が」データの取得や管理をするのかが分かりにくい場合もあるので注意が必要です。

次に、どんなデータが収集されるのかを確認しましょう。あなたが予想していなかったようなデータが収集されている場合があるかもしれません。どんなデータが企業に収集されるのかを理解し、サービスを利用しましょう。

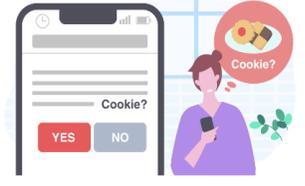
続いて、データの利用目的が説明されている箇所があります。ここでは、収集したデータを企業がどのように利用している

Cookieってなんだろう？

あなたがWebサイトを閲覧したりスマホアプリを利用しようとしたときに、Cookie使用について同意を求めるポップアップが表示されたことはありませんか？

このようなとき、あなたは「同意する」ボタンをクリックしてそのままサイトを閲覧しますか？なぜこのようなポップアップが表示されるのか、同意をする、あるいは同意をしない何が起るのか、疑問に思ったことはありませんか？

今回はCookieとは何か、どのように利用されているのかについてお話ししたいと思います。



CookieはITの進化とともに開発された行動追跡技術のひとつです。私たちのインターネットでの行動を追跡できる技術なので、Cookieがどのような働きをするのか、なぜ利用されるのかを自分自身で理解することはとても重要です。まずはCookieがどのようなものかを見ていきましょう。

Cookieとは、あなたがWebサイトやスマホアプリにアクセスし、提供しているサービスを利用する際に、あなたが利用している端末（PC、スマホ、タブレットなど）に送信される小さなデータファイルのことを指します。

このデータファイルには、あなたの端末を識別するためのデータが記録されていますが、保存されるデータの種類は、Cookieの機能によって異なります。

たとえば、デバイスIDがあります。同じWebサイトに訪問した時、あなたの端末であることを特定できるようにするためのIDがCookieにデータとして保存されています。

この技術を利用することで、同じWebサイトにアクセスする際に何度もログインを行う手間を省くことができます。つまりWebサイトは端末に送信されたCookieのデータを読み取り、Webサイト側で保存されているあなたの他のデータと照合することができるというわけです。

また、ある通販サイトを閲覧していて、ショッピングカートに様々な商品を追加したとします。しかし、時間がなくて「購入」ボタンを押すところまで進むことができませんでした。翌日、改めてサイトにアクセスすると、昨日ショッピングカートに入れた商品が引き続きショッピングカートに残っていますよね。これもCookieを利用した便利な機能のひとつなのです。

Cookieのデータは、Webサイトにアクセスするときに行う言語の選択にも利用されます。あなたの選んだ言語がCookieにデータとして保存されると、同じWebサイトに再度アクセスした時に、改めて言語を選択しなくても、以前に選んだ言語で表示されます。

Cookieに保存されるデータの例としては、閲覧履歴があります。Webサイトの運営者はCookieによって保存されるあなたの閲覧履歴を利用して分析し、Webサイトを改善

- インプリ過程で法解釈について悩むケースあり

(例)

- i 個人関連情報を「個人データとして取得する」の具体的意義は？
- ii QA改定との関係で、7-41の②の「同意」の法的位置づけは？
- ポイント付与のためのデータ連携
- 公式文書（法令、ガイド、QA、パブコメ）での明確な見解

<連携先>

- 個人情報保護委員会
- 経済団体、業界団体
- 他企業
- 弁護士
- 有識者

【参考】

※ガイドライン通則編パブコメ No350 (2021年8月2日)

意見

【該当箇所】 3-7-2-1 「個人データとして取得する」について (93 頁)
【意見】 「提供を受けた個人関連情報を直接個人データに紐付けて利用しない場合は、別途、提供先の第三者が保有する個人データとの容易照合性が排除しきれないとしても、ここでいう『個人データとして取得する』場合には直ちに該当しない」とのことであるが、提供先の第三者が保有する個人データと紐付けて利用するものの、紐づける個人データが、それ単体では個人を識別することができるものではなく、容易照合性の観点から個人データとなっている情報（例：IDのみで管理されている情報）である場合にも、「個人データとして取得する」場合に該当しないとの理解でよいか確認したい。
【理由】 仮に、上記のケースが、提供先の第三者が個人関連情報を個人データとして取得する場合に該当するとすると、事業者が保有する個人関連情報を広告配信プラットフォームに開示し、広告配信プラットフォームにおいて当該個人関連情報と広告配信プラットフォームが保有する個人データ（容易照合性の観点から個人データとなっているものの、それ単体では個人を識別することができないもの）を組み合わせることで広告の拡張配信を行うようなケースや、受け手側として、事業者が保有する氏名等と紐づけることを予定せずに第三者から取得した個人関連情報を取得し、自社のデータベース内に格納するケースにも、個人関連情報の規制がかかることとなってしまうためである。 【経営法友会】

※ガイドライン通則編（個人関連情報に関する説明）

3-7-2-3 同意取得の方法

同意取得の方法としては、様々な方法があるが、例えば、本人から同意する旨を示した書面や電子メールを受領する方法、確認欄へのチェックを求める方法がある。ウェブサイト上で同意を取得する場合は、単にウェブサイト上に本人に示すべき事項を記載するのみでは足りず、それらの事項を示した上でウェブサイト上のボタンのクリックを求める方法等によらなければならない。

また、同意取得に際しては、本人に必要な情報を分かりやすく示すことが重要であり、例えば、図を用いるなどして工夫することが考えられる。

なお、個人関連情報の第三者提供につき、同意取得の一般的なフローについては、本ガイドライン末尾の【付録】を参照のこと。

意見に対する考え方

改正後の法第 26 条の 2 は、個人関連情報の提供先において、個人関連情報を個人データとして取得することが想定される場合に適用されることとなります。
個別の事案ごとに判断することとなりますが、提供先の第三者が、提供を受けた個人関連情報を、それ単体では特定の個人を識別することができない情報と紐付けて利用するのみであり、個人データとして利用しないのであれば、「個人データとして取得する」場合に該当しないと考えられます。

※個人情報保護委員会Q&A

Q 7 - 41 委託に伴って提供された個人データを、委託先が独自に取得した個人データ又は個人関連情報と本人ごとに突合することはできますか。

A 7 - 41 個人データの取扱いの委託（法第27条第5項第1号）において、委託先は、委託に伴って委託元から提供された個人データを、独自に取得した個人データ又は個人関連情報と本人ごとに突合することはできません。

したがって、個人データの取扱いの委託に関し、委託先において以下のような取扱いをすることはできません。

事例 1) 既存顧客のメールアドレスを含む個人データを委託に伴って SNS 運営事業者へ提供し、当該 SNS 運営事業者において提供を受けたメールアドレスを当該 SNS 運営事業者が保有するユーザーのメールアドレスと突合し、両者が一致した場合に当該ユーザーに対し当該 SNS 上で広告を表示すること

事例 2) 既存顧客のリストを委託に伴ってポイントサービス運営事業者等の外部事業者へ提供し、当該外部事業者において提供を受けた既存顧客のリストをポイント会員のリストと突合して既存顧客を除外した上で、ポイント会員にダイレクトメールを送付すること

これらの取扱いをする場合には、①外部事業者に対する個人データの第三者提供と整理した上で、原則本人の同意を得て提供し、提供先である当該外部事業者の利用目的の範囲内で取り扱うか、②外部事業者に対する委託と整理した上で、委託先である当該外部事業者において本人の同意を取得する等の対応を行う必要があります。

(令和 3 年 9 月追加)

Q 1 - 61 同意は、本人の明示的な意思表示を受ける方法によらなければなりませんか。

A 1 - 61 同意は、本人による承諾の意思表示をいいますので、「明示の同意」以外に「黙示の同意」が認められるか否かについては、個別の事案ごとに、具体的に判断することとなります。

おわりに

- ① プライバシーポリシーの位置づけ、わかりやすい説明
- ② 法律の遵守は「最低限」、ユーザの視点
- ③ 社内啓発
- ④ 他社や有識者との連携
- ⑤ 規制当局との連携
- ⑥ 最新ビジネス、テクノロジーの動向把握
- ⑦ 情報セキュリティ部門との連携
- ⑧ グローバルな視点（含：APPIのプレゼンス向上）
- ⑨ プライバシー組織の人的充実化

※社内ポスター

Do you have a new project idea that will use personal data?

Request a **Privacy Investigation!**

What is a Privacy Investigation?

A compliance check by privacy professionals:

- ▶ to avoid violation of privacy laws;
- ▶ to find a consumer friendly solution for you and your customers that builds trust.

When Should I make a request?

In the design phase!

Always involve the privacy team from step one.

How can I request it?

Visit our Confluence GPO

E-mail address...

Rakuten