

STAR Fidélité

En cours

Par Benoit BAUDRIER le 21 septembre 2020

STAR fidélité est un programme de fidélité qui permet de gagner des points cadeaux à chacun des voyages avec la carte KorriGo Services. Les validations sur les trajets quotidiens dans un bus, un métro, à vélo ou en covoiturage donnent droit à des ponts échangeables pour des offres présentes dans la boutique. L'inscription à STAR Fidélité se fait de manière déportée. L'inscription se fait sur le site STAR.fr sur lequel l'utilisateur renseigne prénom, nom, date de naissance, adresse postale, mail, mot de passe, numéro de carte Korrigo, numéro Covoit'STAR et numéro le vélo STAR. L'inscription à STAR Fidélité se fait par l'interrogation d'un webservice de la STAR. Si l'utilisateur renseigne ses identifiants de STAR sur STAR Fidélité et que ceux ci sont corrects, le compte est créé sur STAR Fidélité. A l'inscription, sont récupérées les infos : mail, mdp, nom, prénom, numéro de carte Korrigo, numéro Covoit'STAR et numéro le vélo STAR.

Traitements

Programme de fidélité - IREBY V1

Données

Données traitées

- Caractéristiques personnelles (âge, sexe, état civil...)
 - Date de naissance
- Données d'identification (nom, adresse...)
 - Abonnements mobilité
 - Adresse postale
 - ID Ireby
 - Identifiant client
 - Nom
 - Prénom
- Données d'identification électronique (adresses IP, cookies...)
 - Adresse électronique personnelle
 - Adresse électronique professionnelle
 - Adresse IP
 - Cookies
 - Logs
- Enregistrements d'images
 - Photographie
 - Visuels des offres
- Habitudes de vie
 - Actions de Mobilité
 - Habitudes de consommation
 - Modes de transport
 - Points fidélité
 - Valeurs des offres en point fidélité
- Profession et emploi
 - Nom de l'entreprise
 - Site Internet de l'entreprise

Nombre d'enregistrements

10000

Conservation

1 année après la date de la collecte des données (*supprimées*)

- Données d'identification électronique (adresses IP, cookies...)
 - Logs

10 jours après la date de la collecte des données (*supprimées*)

- Données d'identification électronique (adresses IP, cookies...)
 - Adresse IP
 - Cookies

1 jour après la date de la fin de la relation commerciale (*supprimées*)

- Caractéristiques personnelles (âge, sexe, état civil...)
 - Date de naissance
- Données d'identification (nom, adresse...)
 - Abonnements mobilité
 - Adresse postale
 - ID Ireby
 - Identifiant client
 - Nom
 - Numéro de téléphone privé
 - Prénom
- Données d'identification électronique (adresses IP, cookies...)
 - Adresse électronique personnelle
- Enregistrements d'images
 - Photographie
- Habitudes de vie
 - Actions de Mobilité
 - Habitudes de consommation
 - Modes de transport
 - Points fidélité

Selon le critère suivant **les données des marchands et de leurs offres sont conservées jusqu'à fin du contrat du programme de fidélité avec star. les données sont supprimées de la plateforme sur demande écrite du marchand.**

- Les données des marchands et de leurs offres sont conservées jusqu'à fin du contrat du programme de fidélité avec STAR. Les données sont supprimées de la plateforme sur demande écrite du marchand.
 - Caractéristiques personnelles (âge, sexe, état civil...)
 - Données d'identification (nom, adresse...) (*ID Ireby, Nom, Numéro de téléphone professionnel, Prénom, Raison sociale (Marchand)*)
 - Données d'identification électronique (adresses IP, cookies...) (*Adresse électronique professionnelle*)
 - Enregistrements d'images (*Visuels des offres*)
 - Habitudes de vie (*Valeurs des offres en point fidélité*)
 - Profession et emploi (*Nom de l'entreprise, Secteur d'activité, Site Internet de l'entreprise*)

Transfert

Partenaires

- DRI (*France*)

Sécurité

Mesures de sécurité

- Accès distant
 - Accès VPN (Réseau privé virtuel) ou par un tunnel chiffré
- Application (applications métiers)
 - Contrôle d'accès applicatif
 - Identification des besoins ou exigences de sécurité à mettre en œuvre lors de la conception
 - Mise à jour régulière des applications
 - Prise en compte de règles ou de guides de développement sécurisé
 - Séparation des comptes d'administration et d'utilisation métier de l'application
 - Support applicatif de l'éditeur ou d'une communauté
- Applications Web
 - Mise en place de mesure de gestion des erreurs, de détection d'intrusion et de journalisation
 - Prise en compte de mesure contre l'injection (ex : requêtes paramétrées, encodages des données, validation des entrées)
 - Tests ou audit de sécurité réalisés sur l'application
 - Utilisation des mesures de sécurité des framework éprouvées

- Archivage
 - Archivage logique déconnecté des réseaux
 - Procédure imposant aux utilisateurs de recourir à l'archivage pour les éléments nécessitant d'être conservé sur une période définie
 - Protection de l'intégrité des archives (ex : protection physique ou contrôle d'intégrité logique)
 - Protection de la confidentialité des archives (ex : gestion des accès physique ou logique, chiffrement)
 - Système d'archivage (numériques ou papier) pour la conservation longue d'éléments le nécessitant
- Cryptographie
 - Protection des clés privées
 - Séquestre des mécanismes de restauration des clés
 - Utilisation d'un processus de génération de clés reconnu ou évalué
 - Utilisation de taille de clé suffisante pour le chiffrement
 - Vérification de la révocation des clés
- Destruction
 - Système de destruction (purge automatique ou procédure) des données au-delà des délais de conservation imposés
- Fournisseurs
 - Authentification systématique du fournisseur accédant au système d'information
 - Journalisation des actions menées par les fournisseurs sur le système d'information
- Gestion des accès
 - Authentification par identifiant et mot de passe
 - Authentification par identifiant nominatif
 - Complexité de mots de passe imposée
 - Limitation des accès par groupe, rôle ou profil
 - Mécanisme d'authentification de chaque utilisateur
 - Protection des échanges d'éléments d'authentification en confidentialité et intégrité (ex : hachage des mot de passe)
 - Protection du stockage des éléments d'authentification en confidentialité et intégrité (ex : hachage des mot de passe)
 - Revue des droits d'accès
- Gestion des droits à privilège (ex : droits administration, droits de modification de données ou de configuration, accès distants)
 - Demande formelle pour l'attribution de droits à privilèges
 - Inventaire des droits à privilège
- Infrastructure
 - Durcissement des configurations
 - Mise à jour régulière des équipements de l'infrastructures
- Locaux
 - Les visiteurs sont systématiquement accompagnés
 - Site clos par une enceinte (le périmètre avec l'extérieur est renforcé, ex : clôture robuste, fenêtres au réez de chaussée barricadées, points d'entrée limités au strict nécessaire)
 - Système de contrôle d'accès (automatique ou gardiennage) systématique sur les accès extérieurs
 - Système de détection d'intrusion relié à une équipe de surveillance pouvant intervenir rapidement
 - Zone d'accueil délimitée pour filtrer les visiteurs
- Papiers et support amovibles
 - Politique de bureau propre respectée (ex pas supports de documents confidentiels ou de post-its avec mots de passe laissés sur les bureaux)
 - Règles de sécurité à destination des utilisateurs pour la manipulation de supports physiques de documents confidentiels
- Personnes (ensemble des utilisateurs accédant aux données personnelles (ex : salariés, stagiaires, fournisseurs, partenaires, etc.))
 - Clauses d'engagement sur des règles de sécurité à respecter pour garantir la protection des données personnelles
 - Clauses de confidentialité signées par les personnes accédant aux données personnelles
 - Sensibilisation régulière à la sécurité
- Postes bureautiques
 - Antivirus
 - Authentification au démarrage
 - Verrouillage de session en cas d'inactivité
- Réseau
 - Authentification des équipements autorisé à communiquer sur le réseau
 - Cloisonnement des réseaux par des équipements filtrants
 - Cloisonnement physique des réseaux
 - DMZ ou zone démilitarisée avec les réseaux extérieurs
 - Filtrage applicatif (Pare feu applicatif, Proxy)
 - Filtrage réseau (ex : Pare-feu, routeurs filtrants)
 - Procédure de demande d'ouverture de règles de filtrage
 - Revue des règles de filtrages
 - Utilisation de protocoles sécurisés (ex : HTTPS, SFTP, SSH)
- Réseau sans-fil
 - Les algorithmes pour l'accès au réseaux wifi respecte l'état de l'art et (ex : WPA2, WPA-Entreprise)

- Sauvegarde
 - Contrôle des sauvegardes (reprise, redémarrage)
 - Externalisation de copie des sauvegardes
 - Protection des données sauvegardées avec le même niveau de sécurité que les données sur l'infrastructure
 - Sauvegarde des données
- Stockage des données
 - Anonymisation des données
 - Chiffrement des données
 - Contrôle d'intégrité des données (ex : mécanismes cryptographiques, solution de scellement)
- Surveillance
 - Des procédures permettent aux équipes d'intervention de réagir efficacement (ex : instructions, fiches réflexes) en cas d'alerte
 - Génération d'alerte en cas d'élément de sécurité vers l'équipe d'exploitation
 - Les journaux (logs) sont protégés contre la modification et la destruction
 - Mécanisme d'analyse des journaux (logs)
 - Mécanisme de surveillance en temps réel d'évènement anormaux ou illicites
 - Présence d'une équipe permanente ou disponible sur appel (astreinte) en cas d'alerte
- Traitement
 - Contrôle de cohérence des données après traitement
 - Contrôle de saisies des données (ex : format, fourchette, min, max)
 - Imputation des données saisies ou modifiées à son auteur
- Transfert de données
 - Chiffrement des données lors des échanges
 - Chiffrement des échanges sur les réseaux
 - Garantie de l'origine de la donnée du correspondant avant tout transfert des données (en émission ou en réception)
 - Garantie de l'origine de la donnée en réception
 - Mécanisme anti rejeu des messages (numérotation, séquençement) protéger contre la modification

Clients de la prestation

Clients

- STAR (Kéolis RENNES)

Propriétés complémentaires

 Aucune propriété complémentaire

Acteurs

 Aucun acteur n'a été défini

Pièces justificatives

Date

Nom

Taille

 Aucune pièce justificative

Version



27 oct. 2021 à 15:44

Version courante



Philippe CHUSSEAU 27 mai 2021 à 17:20



Benoit BAUDRIER 21 sept. 2020 à 17:36

Création