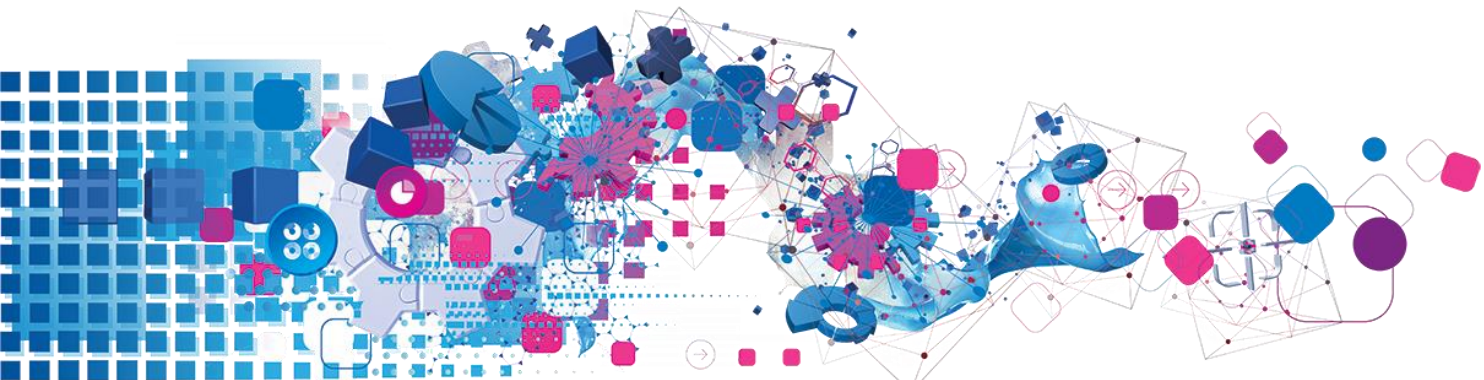
Email Validation



Contents

Email Validation

1. About the product

Experian's cloud-based email validation tool removes bad email addresses at the point of capture to improve your sender reputation, increase deliverability and ensure your communications reach your citizens.

2. Product Features

Superior technology to identify invalid emails
Corrections logic to identify misspellings and typo traps
Clear, actionable response codes
Flexible integration options
Pre-validation syntax check to ensure the email is well-formed
Experian's trusted secure data and privacy standards
99.9% uptime Service Level Agreement
Robust and secure infrastructure
Active validation of the email by communication with each ISP

3. Product Benefits

Improved data integrity for better decision making
Accelerated processes for improved citizen experience
Decreased IT costs from using cloud based service
Improved operational efficiencies
Better communication with citizens by ensuring your messages arrive efficiently

4. Service Scope

4.1 Software add-on or extension

No

4.2 Cloud deployment model

The software is hosted by Experian Data Quality on its SaaS platform.

4.3 Service constraints

No however if we do have any planned improvements which we believe will materially affect your service, we will contact you.

4.4 System Requirements

Fully supported release of web browser

5. User Support

5.1 Email or online ticketing support

Email or online ticketing

5.2 Support response times

Responses are provided within 24 hours

5.3 User can manage status and priority of support tickets

No

5.4 Phone support

Yes

5.5 Phone support availability

09:00 to 17:00 (UK time), Monday to Friday

5.6 Web chat support

Web chat

5.7 Web chat support availability

09:00 to 17:00 (UK time), Monday to Friday

5.8 Web chat support accessibility standard

WCAG 2.0 AAA

5.9 Web chat accessibility testing

Constant review/enhancement of user journey to ensure case resolution provided via chat

5.10 Onsite support

Yes, at extra cost

5.11 Support levels

We do not operate a differentiated service model (i.e. no gold, silver, bronze levels of access)

5.12 Support available to third parties

Yes

6.0 Onboarding and offboarding

6.1 Getting Started

Full user guides available, welcome product calls, online FAQ and video content, plus paid-for integration assistance available

6.2 Service documentation

Yes

6.3 Documentation formats

PDF

6.4 End-of-contract data extraction

Data is retained by Experian Data Quality for up to 90 days for internal diagnostics, caching and reporting purposes. (Customer data is not shared with anyone outside of Experian.)

6.5 End-of-contract process

At the end of the contract, the Buyer shall cease to use all Licensed Materials and Licensed Programs

7.0 Using the service

7.1 Web browser interface

This product does not have an externally accessible graphical interface. The only way to interface with it is via an API.

7.2 Supported browsers

Not applicable

7.3 Application to install

Not applicable

7.4 Compatible operating systems

Not applicable

7.5 Designed for use on mobile devices

No

7.6 Accessibility standards

None or don’t know

7.7 Description of accessibility

-

7.8 Accessibility testing

This software does not require an installation, as it is an Experian hosted product.

7.9 API

Yes

7.10 What users can and can’t do using the API

Full service functionality provided via API

7.11 API documentation

Yes

7.12 API documentation formats

Open API (also known as Swagger)

HTML

7.13 API sandbox or test environment

No

7.14 Customisation available

Yes

7.15 Description of customisation

Integration into own environment - requires relevant code language knowledge

8.0 Scaling

8.1 Independence of resources

Full load balancing, multiple data centres

9.0 Analytics

9.1 Service usage metrics

Yes

9.2 Metrics type

Usage metrics are partially available across software suite. the describe usage levels, click balance and service availability

9.3 Reporting types

API access

10.0 Resellers

10.1 Supplier type

Not a reseller

11.0 Staff security

11.1 Staff security clearance

Other security clearance

11.2 Government security clearance

None

12.0 Asset Protection

12.1 Knowledge of data storage and processing locations

Yes

12.2 Data storage and processing locations

This product uses US-based Experian data centres

12.3 User control over data storage and processing locations

No

12.4 Datacentre security standards

Complies with a recognised standard (for example CSA CCM version 3.0)

12.5 Penetration testing frequency

Less than once a year

12.6 Penetration testing approach

In-house

12.7 Protecting data at rest

Physical access control, complying with another standard

12.8 Data sanitisation process

No

12.9 Equipment disposal approach

In-house destruction process

13.0 Data importing or exporting

13.1 Data export approach

This product does require you to import the data to Experian’s platform for batch processing (not real-time).

13.2 Data export formats

Other

13.3 Other data export formats

N/A

13.4 Data import formats

Other

13.5 Other data import formats

N/A

14.0 Data-in-transit protection

14.1 Data protection between buyer and supplier networks

TLS (version 1.2 or above)
Other

14.2 Other protection between networks

SOAP endpoint sslv3/tls1.0/1.1/1.2
REST endpoint TLS1.2

14.3 Data protection within supplier network

TLS (version 1.2 or above)
Other

14.4 Other protection within supplier network

SOAP endpoint sslv3/tls1.0/1.1/1.2
REST endpoint TLS1.2

15.0 Availability and resilience

15.1 Guaranteed availability

We guarantee 99.9% service availability

15.2 Approach to resilience

Automated global failover of product

15.3 Outage reporting

We will notify you of any material outages, that may affect you, by email.

16.0 Identity and authentication

16.1 User authentication needed

Yes

16.2 User authentication

Username or password
Other

16.3 Other user authentication

Secure token

16.4 Access restrictions in management interfaces and support channels

-

16.5 Access restriction testing frequency

At least once a year

16.6 Management access authentication

Username or Password

17.0 Audit information for users

17.1 Access to user activity audit information

No audit information available

17.2 Access to supplier activity audit information

No audit information available

17.3 How long system logs are stored for

At least 12 months

18.0 Standards and Certifications

18.1 ISO/IEC 27001 certification

Yes

18.2 Who accredited the ISO/IEC 27001

DNV GL Business Assurance Limited

18.3 ISO/IEC 27001 accreditation date

20/12/2016

18.4 What the ISO/IEC 27001 doesn’t cover

The following is covered by the scope of the certificate; the delivery and support of Experian IT infrastructure, operations, architecture and associated compliance and facilities management undertaken within the UK data centres.

18.5 ISO 28000:2007 certification

No

18.6 CSA STAR certification

No

18.7 PCI certification

No

18.8 Who accredited the PCI DSS certification

Trustwave

18.9 PCI DSS accreditation date

28th October 2016

18.10 What the PCI DSS doesn't cover

Everything is covered

18.11 Other security certifications

No

19.0 Security Governance

19.1 Named board-level person responsible for service security

Yes

19.2 Security governance certified

Yes

19.3 Security governance standards

ISO/IEC 27001

19.4 Information security policies and processes

Experian has a comprehensive global security policy based on the ISO27001 standard which covers: Organisation and Management, information security, asset classification, physical and environmental security, communications and operations management, system access, systems development and maintenance, compliance, personnel and provisioning, business continuity management, third party management. The policy is owned by Experian's executive risk management committee which is an executive level body, and which assumes ultimate responsibility for Experian's risk position. Information security is a key component of the risk management framework. Experian management supports security through leadership statements, actions and endorsement of the security policy and implementing/improving the controls specified in the policy. The policy is available to all Experian employees and contractors on the intranet. Changes to the policy are announced on the company's intranet computer based information security and data protection training, and this is repeated on at least an annual basis. Compliance to policy is overseen by internal audit.

20.0 Operational security

20.1 Configuration and change management standard

Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

20.2 Configuration and change management approach

Experian has a change management policy which is underpinned by processes and procedures based on ITIL best practice. This is a mature process. We use a service management tool that integrates change management, incident management, problem management, configuration management and knowledge management. Our change management policy, processes, and

procedures are regularly audited by independent auditors. Formal risk analysis is employed using an approved information risk analysis phase for developments/changes. Security requirements for the system are identified and continue to be considered throughout the life of the product.

20.3 Vulnerability management type

Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

20.4 Vulnerability management approach

Servers are built to a documented secure standard, which includes anti-virus and malware defences. Information assets have a defined patching schedule, determined by the system's criticality and the level of threat the patch is mitigating. Experian actively monitors threat environment and checks the effectiveness of security controls by reviewing both free and paid for sources of threat information, including, public information, major vendor feeds and receiving information from specialist closed group mailing lists. The overall process is also plugged into an automated patch and fix strategy, underpinned with a technology infrastructure to deliver corrective updates.

20.5 Protective monitoring type

Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

20.6 Protective monitoring approach

Monitoring processes and tools are in place to manage alarms generated by security related alerts and these are fed into the incident management process. Experian has a formally documented risk based incident management process to respond to security violations, unusual or suspicious events and incidents. In the event an incident occurs a team of experts from all relevant areas of Experian are gathered to form an incident response team, who manage activities until resolution. The incident response team are available 24/7 to resolve any incident. Out of core hours the dedicated incident hotline is routed to the command centre

20.7 Incident management type

Conforms to a recognised standard, for example, CSA CCM v3.0 or ISO/IEC 27035:2011 or SSAE-16 / ISAE 3402

20.8 Incident management approach

The incident management process incorporates a number of participants and contributors, including: Global Security Office - who facilitate and coordinate activities under the business security coordinator's guidance; Business Security Coordinator - a representative of the impacted business area, responsible for coordinating resolution activities; Incident Response Team (IRT) - IRT is made up of a membership that are empowered to make key decisions surrounding the actions to be taken to reduce impact, control actions, and impose corrective activities. A client report would be created, including: high level overview; facts; overview of events; actions taken.

21.0 Secure development

21.1 Approach to secure software development best practice

Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v3.0)

22.0 Public service networks

22.1 Connection to public service networks

No

23.0 Pricing

23.1 Price

£0.002 per transaction

23.2 Discount for educational organisations

No

23.3 Free trial available

Yes

23.4 Description of free trial

Free trials can be provided to Buyers for a maximum period of three months. During this period, the Buyer will have full functionality and where transactions are provided, transactions will be limited to 500 lookups. The trial is only for demonstration purposes and cannot be used in a live environment.

24.0 Documents

24.1 Service definition document

https://assets.digitalmarketplace.service.gov.uk/g-cloud-10/documents/700542/233966377957179-service-definition-document-2018-05-17-1027.pdf