

## ACCEPTABLE USE POLICY (AUP) FOR CONFIRMIT SODA SOFTWARE v3.4

---

### END-OF-LIFE NOTIFICATION

Confirmit SODA Software Version 3.4.n, where n increments with each new Updates or Upgrades, is now a Frozen Version. The latest available Frozen Version continues to be a supported version, but it is no longer under active development. Client is encouraged to upgrade to Confirmit Horizons which offers significant benefits and ongoing Updates and Upgrades. CONFIRMIT may issue Updates or Upgrades to supported Frozen Versions of Confirmit SODA, provided however that such Updates or Upgrades will primarily address critical software errors and security vulnerabilities, and will not include new features, and provided that such Updates or Upgrades do not require unreasonable efforts to implement. CONFIRMIT shall provide at least one year's notice in writing (email to the Designated Support Contact will suffice) before withdrawing all support for Confirmit SODA. Irrespective of the Term of this Agreement, after support for Confirmit SODA is withdrawn, CONFIRMIT shall be released from its obligations under this Agreement in relation to Support Services, Updates and Upgrades, and the Limited Warranty made by CONFIRMIT in this Agreement shall be void.

---

#### 1. AUP INTRODUCTION

- 1.1. The main objectives of this AUP are to provide CONFIRMIT Clients with reliable and stable access to the Confirmit SODA Software accessed On-Demand (the "Service").
- 1.2. While it is not our intent to actively monitor your use of the Service, we may take such actions as deemed appropriate by us when we become aware of a violation of this AUP.
- 1.3. This AUP supplements, but does not supersede, the Documentation, as well as the agreement that your company has executed with any CONFIRMIT company (the "Agreement"). If the Documentation or the Agreement restricts the use of the Service in areas not addressed in this AUP, the Documentation or the Agreement will govern with respect to such areas.

#### 2. PROHIBITED USE

##### 2.1. Illegal and Criminal Activity / Security Violations / Threats

You may not use the Service to engage in illegal, abusive, or irresponsible behavior, including but not limited to:

- 2.1.1. criminal or civil violations of state, federal, or international laws, regulations, or other government requirements where such violations include but are not limited to theft or infringement of copyrights, trademarks, trade secrets, or other types of intellectual property; fraud; forgery; theft or misappropriation of funds, credit cards, or personal information;
- 2.1.2. unauthorized access to or use of data, services, systems or networks, including any attempt to probe, scan or test the vulnerability of either the Service or another system or network or to breach security or authentication measures, without express prior written authorization of the owner of the system or network;
- 2.1.3. interference to the Service or any user, host or network including, without limitation, mail bombing, flooding, and deliberate attempts to overload a system;
- 2.1.4. use of an Internet account or computer without the owner's authorization;
- 2.1.5. collecting information by deceit, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;
- 2.1.6. use of any false, misleading or deceptive TCP-IP packet header or any part of the header information in an email or a newsgroup posting;
- 2.1.7. use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- 2.1.8. any activity or conduct that is likely to result in retaliation against the Service or us;
- 2.1.9. introducing intentionally or knowingly into the Service any virus, contaminating program or script code; or fail to use an up to date virus-scanning program on all material downloaded from the Services;
- 2.1.10. transmission of materials of threatening nature, including threats of death or physical harm, harassment, libel, racism, sexual or religious discrimination, and defamation; or
- 2.1.11. any other activity or conduct that unreasonably interferes with the Service, or other customers' use of our Service.

##### 2.2. Offensive Content

You may not publish, display or transmit via the Service any content that we reasonably believe to be:

- 2.2.1. unfair or deceptive under the consumer protection laws of the applicable jurisdiction, including chain letters and pyramid schemes;
- 2.2.2. defamatory or violates a person's privacy;
- 2.2.3. creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or
- 2.2.4. interferes with an investigation by law enforcement bodies;
- 2.2.5. improperly exposes trade secrets or other confidential or proprietary information of another person;
- 2.2.6. intended to assist others in defeating technical copyright protections;
- 2.2.7. infringes another person's trade or service mark, patent, or other property right;
- 2.2.8. discriminatory in any way, including by way of sex, race, or age discrimination;
- 2.2.9. constitutes or encourage child pornography or is otherwise obscene, sexually explicit or morally repugnant;
- 2.2.10. facilitates any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive or menacing;
- 2.2.11. excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
- 2.2.12. involves theft, fraud, drug-trafficking, money laundering or terrorism;
- 2.2.13. otherwise illegal or solicits conduct that is illegal under laws applicable to you or to us; and
- 2.2.14. otherwise malicious, fraudulent, or may result in retaliation against us by offended viewers.

"Publish, display or transmit via the Service" includes web content, email, and any other type of posting, display or transmission, direct or by means of references, that relies on the Internet.

### 2.3. Copyrighted Material

You may not use the Service to publish, distribute, or otherwise copy in any manner any text, music, software, art, image or other work protected by copyright law unless you:

- 2.3.1. have been expressly authorized by the owner of the copyright for the work to copy the work in that manner; and
- 2.3.2. are otherwise permitted by copyright law to copy the work in that manner.

### 2.4. Emailing and Spam

- 2.4.1. The Service may only be used to perform the following types of email survey invitations:
  - 2.4.1.1. invitations to surveys actually hosted on the Service (except where otherwise agreed to by us in writing), and reminders thereof;
  - 2.4.1.2. thank-you emails sent upon completion of a survey hosted on the Service;
  - 2.4.1.3. emails automatically generated as a result of respondents completing surveys ("sendmail" scripts);
  - 2.4.1.4. dispatching of exports (data-files or graphical reports) from surveys hosted on the Service
- 2.4.2. The laws and rules applicable to your company will depend on the laws in the jurisdictions to which emails are being sent by you, and include e.g. CAN-SPAM Act of 2003 in the US, or the European Directive 2002/58/CE of 12 July 2002 on privacy and electronic communications. Following are some (but not all) activities that are strictly prohibited:
  - 2.4.2.1. sending unsolicited or undesired email messages ("spam")
  - 2.4.2.2. sending email without providing in the email itself a simple way of requesting to be excluded from receiving additional emails from the originator of the email ("opt out");
  - 2.4.2.3. sending emails that do not accurately identify the sender's name, the sender's return address, and the email address of origin, or in general misrepresenting oneself;
  - 2.4.2.4. sending email for the primary purpose of commercial advertising or promotion, independent of whether a Confirmit SODA survey is referred to or used;
  - 2.4.2.5. sending email with charity requests, petitions for signatures, or any chain mail related materials; and
  - 2.4.2.6. collecting the responses from unsolicited email.

### 2.5. Text Messages, Short Message Service (SMS), and Push Notifications

- 2.5.1. The Service may only be used to perform the following types of text message survey invitations:
  - 2.5.1.1. invitations to surveys actually hosted on the Service (except where otherwise agreed to by us in writing), and reminders thereof;
  - 2.5.1.2. thank-you text message sent upon completion of a survey hosted on the Service;
  - 2.5.1.3. text message automatically generated as a result of respondents completing surveys ("sendmail" scripts);
- 2.5.2. The laws and rules applicable to you will depend on the laws in the jurisdictions to which text messages are being sent by your company. Following are some (but not all) activities that are strictly prohibited:
  - 2.5.2.1. sending unsolicited or undesired text messages ("spam")
  - 2.5.2.2. sending text messages for the primary purpose of commercial advertising or promotion, independent of whether a Confirmit SODA survey is referred to or used;
  - 2.5.2.3. sending text messages with charity requests, petitions for signatures, or any chain mail related materials; and
  - 2.5.2.4. collecting the responses from unsolicited text messages.

## 3. REGULATIONS ON USAGE OF CONFIRMIT SOFTWARE ON-DEMAND

### 3.1. Data collection, emailing, text messaging

- 3.1.1. Unless agreed differently in writing with us, the total survey activity generated by your company across any and all projects hosted on the Service shall not be above the thresholds listed below. Where you need to exceed the stated thresholds, then at least 5 business days prior to the planned release day of the survey, you must apply to exceed the limits by sending an email request to support@confirmit.com. A "High Capacity" fee may be applicable.

Responses Uploaded:	Max 25,000 per day
Response Files (*) Uploaded:	Max 25,000 per day
Response Files Total Size:	Max 5GB per day - (based on 25,000 files @ 200kb each)
Emails Sent:	Max 10,000 per day
Text Messages Sent:	Max 1,000 per day
Push Messages Sent:	Max 10,000 per day

(\*): A response file is any captured media file (photo, video, audio)

- 3.1.2. It is your company's responsibility to ensure that the number of emails sent does not exceed the total responses desired for the project.
- 3.1.3. We cannot provide any guarantees relating to deliverability, or to delivery times, of emails, text messages or push messages sent from the Service.

### 3.2. Survey Design

- 3.2.1. Although we have designed the Service to handle data collection and reporting strain generated by the most advanced activity of our clients, extreme use may cause performance issues or errors. We shall not be responsible for issues relating to extreme use. Please see the following limitations for survey design:

General	Recommended Limit	Reason
Forms	5,000	Device performance
Variables	50,000	Device performance
Form Label text length	8,000 characters	System
Category Lists	1,000	Device performance
Category Items per Category List	2,000	Device performance
Category Item text length	8,000 characters	System

Form Script length (per event script)	32,000 characters	System
Resource Files	500	Download speed
Total Resource File Sizes	10 MB	Download speed
Dynamic List Resource File Data Rows	10,000	Device performance
Questions in single form (compounded)	25	Device performance
Form Group Max Loop Iterations	1000	Device performance
Device variables ( ie. setSetting() )	1000	Device performance
Variable string length (form, device, etc)	2000	System

“Variables” are determined by:

a) the number of looped forms.

b) the type of form such as multiple response questions: multiple numeric, text, sliding scale, grids, etc. where each row item is considered a variable.

“Reason”:

Device performance – user experience may be affected if this is exceeded based on a typical mobile device.

Download speed – will affect the time it takes to download a project and depending on the quality of connection, could limit the project from being downloaded successfully.

System – This is a hard system limitation. Where possible, a warning will be provided but in some cases a warning may not be possible

Media Capture	Default	Recommended Limit
Media Capture Questions per survey (photos, videos, audio capture)	N/A	5
Photo Capture Size	640 x 480	640 x 480
Audio Capture Length	1 minute	5 minutes
Background Audio Capture	N/A	5 minutes
Video Capture Length (*)	1 minute	5 minutes

(\*): Restricting length of video capture is not supported on many devices.

**NOTE:** As the survey is executed on various mobile platforms with significantly different resources, these recommended limits are much lower than technically possible using the software. If a survey design requires larger limits, it is your responsibility to perform testing on the designated mobile platform.

### 3.3. SODA Mobile Usage

3.3.1. Although we have designed the SODA Mobile application to handle the most advanced activity of our clients, extreme use may cause performance issues or errors. We shall not be responsible for issues relating to extreme use. The following recommended limits apply to the SODA Mobile application running on a supported mobile device. Please see the following limitations for the SODA Mobile application:

	Recommended Limit
Surveys/Projects assigned or downloaded	50
Completed surveys stored (not yet uploaded) per project	250
Captured Media files stored (not yet uploaded) per project	250
Preloaded surveys (e.g. back-checking) per project	100

**NOTE:** As the survey is executed on various mobile device platforms with significantly different resources, these recommended limits are typically much lower than technically possible using the software. If a survey design requires larger limits, it is your responsibility to perform testing on the designated mobile platform.

### 3.4. Data Exporting and Import

3.4.1. The Service supports various data processing operations, such as: (i) Data Export; and (ii) Data Cleaning. We shall not be responsible for issues relating to extreme use of such features. What would be considered as extreme use will depend on the data processing operations performed and the volumes of data being processed. The following are general guidelines on the limits for the various data processing tasks, based on data sets of different sizes:

Response Data Export	Record Limit	Column Limit
Microsoft Excel 2007	50,000	100,000,000
Microsoft Excel 97-2003	50,000	4,000,000
IBM SPSS	50,000	6,000,000
Delimited File (tab or comma)	50,000	100,000,000
SODA XML	50,000	100,000,000

- A record is defined as any response, whether it is a "complete" or not
- Column Limit is calculated by the number of responses (rows) to be exported by the number of columns required.
- A column may consist of one per variable or multiple in the case of a multiple response question where each possible answer needs to be exported in a separate column for reporting purposes.

Response Data Media Files	File Size (MB)
Captured Media Files Export	1024

NOTE: The above Record and Column limits may be adjusted as required on the SODA SaaS site as the situation warrants.

If any of these limitations mentioned above are exceeded the client is responsible for reducing the size. The size can be reduced by using the SODA Designer.

We reserve the right to take reasonable steps to maintain acceptable performance on the Service. Such steps may include the abortion of tasks. You will normally be informed in advance of any proposed action, and you will reasonably co-operate with us during such process.

### 3.5. Web Services

- 3.5.1. External web service requests that export data or query for a result set are limited to one request every 10 minutes per project.
- 3.5.2. External web service requests that insert/update/delete a single object item (e.g. assignProject) are limited to 50,000 requests per day for any single company account.

### 3.6. System Monitoring

- 3.6.1. We do not permit 3rd party systems to monitor the status of our On-Demand environments, unless we have provided our prior approval.

## 4. CONSEQUENCES OF (i) PROHIBITED USE, AND (ii) REGULATIONS OF USAGE

- 4.1. Violations by you, including use by your customers, of the regulations in Articles 2 and 3 of this Schedule may result in (i) immediate removal of offending materials; (ii) blocked access to, or partial or full suspension of Service; or (iii) other reasonable actions appropriate to address the violation, as determined by us in our sole discretion. We shall make reasonable efforts to contact your company so that violations may be addressed voluntarily by your company, however we do reserve the right to act without notice when necessary to preserve the stable, secure and uninterrupted operations of the Service, as determined by us in our sole discretion.
- 4.2. You may be requested by us to bring the offending or breaching materials in compliance with this AUP and the Agreement. Any costs incurred by you in conjunction with this shall be borne solely by your company.
- 4.3. We may involve, and will cooperate with, law enforcement agencies and government agencies if criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law.
- 4.4. With the exception of our gross negligence or willful misconduct, we shall have no liability whatsoever to your company in connection with actions taken by us in response to your violation of this AUP. Furthermore, you shall not be entitled to any compensation under the Service Level Agreement if the cause of the issue is a breach of the AUP by you.
- 4.5. We will charge you at our standard rates for Additional Services for work necessitated by us and related to breaches of the AUP by your company. Charges will be applied reasonably, but repeated offences will be charged in full. Charges may e.g. apply when we are to (i) investigate or otherwise respond to any alleged or actual violation of this AUP by you; (ii) remedy harm caused to us or to any of our other customers by your use of the Service in violation of this AUP or the Agreement; (iii) respond to third party complaints related your use of the Service in breach of the AUP; and (iv) work related to removal our Internet Protocol numbers from any "blacklist" in the wake of your actions.

## 5. INCIDENT REPORTING

- 5.1. Any complaints regarding violations of this AUP should be directed to abuse@confirmit.com, and where possible, include details that would assist us in investigating and resolving the complaint.

## 6. REVISIONS OF THIS AUP

- 6.1. We may modify this AUP at any time with thirty (30) days prior email notification to Designated Users. Such modifications will be effective when posted to our public web site, or extranet web site.

## General recommendations when sending email invitations from the Service

To assist you in complying with the laws and regulations that prohibit 'spam' in email messages (e.g., CAN-SPAM Act of 2003 in the US and the European Directive 2002/58/CE of 12 July 2002 on privacy and electronic communications) Confirmit has prepared the following recommendations. **These are not a substitute for independent legal and regulatory advice obtained from your own advisors based on the situation, the specific circumstances and the particular jurisdictions, laws and regulations that apply.**

Generally, the laws in the US, Europe and other jurisdictions prohibit sending unsolicited or undesired email or "spam." Most also require there be a notice and working mechanism (e.g., link) in the email to enable the recipient to "opt out" – to request exclusion from receiving additional emails from you. These laws also generally prohibit sending emails that do not accurately identify the sender's name, return address and the email address of the originator of the email and generally prohibit misrepresenting one's identity. Furthermore, these laws usually prohibit sending email for the primary purpose of commercial advertising or promotion, whether or not you are using or referring to a Confirmit survey, without consent and also restrict the use of email for soliciting charitable donations, petitions for signatures, chain emails or collecting responses from unsolicited email.

Here are some recommendations based on our experience:

1. Avoid using "spam" related terms as a teaser in the subject field (e.g. "win", "chance to win", "get paid to respond").
2. Avoid ambiguity - in the subject heading field clearly identify the non-sales/non-marketing reason the individual is being contacted by

email.

3. Be transparent - tell the recipient how you obtained access to his/her email address: For example:
  - "We at <company> are contacting our clients for this satisfaction survey."
  - "You are receiving this invitation because you have joined the <company> panel."
  - "We at <company1> have been asked to perform this study on behalf of <company2>, who provided your email address to us."
4. Include opt-out information in the email e.g.: "If you do not wish to receive further invitations from us to participate in surveys, please send an email to <email address> or click the following link <link>. It may take up to <number> days to process your request. If you receive further invitations or reminders during that period, please disregard them.". Make sure the opt out procedures work
5. Include a link to your Privacy Policy which clearly sets out how data that is collected will be used, how you intend to maintain anonymity of respondents. You should do so either in the Invitation email or at the beginning of the survey. We also recommend including a link to your Privacy Policy on every page of your questionnaire (easily achieved by including the link in the Web Interview template).
6. You must clearly and accurately identify the company and person sending the email, including your company's physical address.

Useful links in relation to the above are

- <http://business.ftc.gov/documents/bus61-can-spam-act-Compliance-Guide-for-Business>.
- <http://www.esomar.org/knowledge-and-standards/codes-and-guidelines/guideline-for-online-research.php>, see #2.2.1 in particular.