Absowebly SaaS solutions - On Approach to GDPR (May 2018)

This update is giving you - the Absowebly customer insight into how we are going to address the latest changes in the legal approach to the privacy policies, security and sharing of the personal data that will be in force from 25th May 2018. The legislation was passed two years ago as a REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) - in short GDPR (you can study the text of the regulation in full here).

Please note this document is neither a piece of advice on how to deal with GDPR, nor it attempts to explain GDPR.

We are not advisors on the matter of private data handling. This document only explains what actions we at Absowebly take in relation to the regulation to make sure we, as a data processor, are ready for implementations of data protection elements in our processes. It explains what you can expect from us on the matter of GDPR implementations and communication but also to acknowledge what we expect from you. It is in your interest as a data controller to read it as we establish particular processes and schedules related to GDPR implementations on our side.

To understand your statutory obligations regarding GDPR, you need to go to the ICO's website and read the original text of the regulation.

We believe our five-chapter update replies to the relevant parts of the regulation in the aspect of our responsibility as a web software provider (data processor) to your company (data controller).

1) Our work and the general information and setting of the GDPR and how we see it.
2) The most popular question – What about cookies?
3) Collect as little data as possible to process and share it with as few third parties as possible
4) Right to be forgotten – right to erasure and how Absowebly complies
5) Security by design - encryption and notifications

1) GDPR concepts and our cooperation with you as a data controller

Please note in all regulations there is a lot of room for interpretation, and over the last weeks, we have seen a lot of comments and behaviours that claim things that are not in the act itself but are part of some specific interpretation of the law.

In the legal manual among 173 notes to GDPR, The European Parliament and The Council of The European Union mentioned very clearly several things that are related to our trade and stated why the specific law had been put in place:

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

So why it is in place from the business web software perspective?

We all have heard about spectacular data losses by our utility companies or government departments where a single person had access to millions of records of citizens that were carried on the USB stick and left on a train without any encryption. Possibly you experienced a lack of responses of some companies to requests for data that they stored on you indefinitely and without checking the accuracy of that data. From time to time media reports cases where enigmatic entries on credit agencies records combined with bank mistakes allow to start the process of home repossession or other legal actions. We are also all subject to day to day consent tricks while browsing the web, with multiple tick boxes confusing us greatly:

- tick to agree,
- tick to disagree,
- untick to agree,
- untick to disagree

(…)

Often all in this same form.

Some people took on companies like Google or Facebook and went through a long journey of high profile court cases for the "right to be forgotten".

To catch up with all these elements and other society changing behaviours GDPR had been put together as a common-sense based legal hub for guidance, policing and directions related to managing private individual data. It is a legal document strongly influenced by court cases and other events of the first 15 years of the 21st century and creates a modern platform that in the core:

a) tries to restrict what data is passed for processing in the general assumption “less is better” – if data is not necessary to collect for your operations – don’t do it! This rule has always been the core of Absowebly processes, and there are no general compliance concerns in this area thanks to the customised approach we took very early.

b) It makes a distinction between hypersensitive, sensitive and less sensitive data. The new regulation tries to enforce the use of some form of security on the data – encryption, tokenisation etc. as well as to create a physical guardian of data (DPO - Data Protection Officer) in case you are dealing with sensitive or hypersensitive data or your volume of data processing is big enough to justify special measures. The core of Absowebly current policy is that we do not deal with hypersensitive and sensitive data in the software design stage. All these elements we try to push for processing to specialist organisations, for example, online credit card payment gateways).

c) It allows subjects of data gathering (individuals) to control transparently, what information, how and when is stored about them.

d) It gives subjects a clearer understanding of why data is gathered and removes confusions from the earlier interpretation of some processes. If you use the Absowebly software, you know that number of ticks in the form processing has always been limited, and we always opted for at least default privacy policy, terms of service and other legal processing elements.

e) It puts a responsibility on data controller to develop systems the way that, by default, they serve the highest level of data protection - "data protection by design". Please note it was always Apsowebly's core idea as a system that is restricting access to data not only internally but by giving power to you – our customer, to distinguish what data is visible where.

f) It puts on cooperation between us (the data processor and you - the data controller) more emphasis and gives us clear timeframes to deal with situations that create a request from the individual or a security problem related to the data.

How exactly our terms and conditions, as well as mechanisms on our software, are going to work with GDPR, please find out below.

2) Cookies - general individual's rights and explicitly consents

In the last couple of years, we had several legal changes to what you should do when you set up cookies on someone's device, and these were widely interpreted as completely different actions by different developers. GDPR only mentions cookies once, and this is in the comment points from the legal manual:

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

That note defines cookies as a privacy identification element, and that definition puts cookies directly in focus of GDPR as cookies defined this way interact directly with six out of eight rights for Individuals:

- the right not to be subject to automated decision-making including profiling;
- the right to be informed;
- the right of access;
- the right to erasure;
- the right to restrict processing;
- the right to object;

  and indirectly with the two remaining

- the right to data portability;
- the right to rectification.

For that reason, you need to:

i) clearly inform your user about intent to gather information about them (set the cookie)

ii) let them easily manipulate that setting (as easy as it was to set the cookie it must be to unset it)

iii) make it clear what that information from particular cookie is used for (inform about what cookies are set and what are the purposes of these)

iv) show precisely for how long it will be used for (information for how long they are set for)

GDPR does not specify what techniques should be used for the display of the message or what mechanisms are used for that. There are several organisations that can help to narrow down some mechanisms (The European Union Agency for Network and Information Security, Information Commissioner's Office etc.) but ultimately the law is constructed the way that allows data controllers to apply technology that fits their individual settings where you can narrow down processes.

In the last few weeks we were working on our software cookies structure, and we simplified it to deal with the GDPR more efficiently. Our mechanisms for cookie settings will be equipped with a new text and are going to follow the structure that allows addressing all individual's rights (GDPR becomes enforceable on 25th May 2018, and all changes will be implemented by this date).

It is worth to say that in general there are two types of cookies out there. Tracking cookies for marketing purposes and cookies that track your actions to make your life easier or to allow you to use specific functionality (for example they allow you to explore websites safely and in an efficient way). This latter type of cookies is often used on websites to store information from your shopping basket, so you can continue to browse website while your items await checkout, a cookie may allow you to watch content, give or withdraw consent regarding different actions on government or public organisation websites etc.

Absowebly’s software sets up both types of cookies:

- necessary/essential cookies for all those who log in to their admin panels, special areas, use shopping carts etc.
- non-essential/tracking cookies these are important for monitoring of web service performance, and marketing and these allow you to manage resources better. Tracking cookies do not need to be present for the individual to conduct a transaction

Essential cookies work the way that withdrawing consent to set them up would make web service impossible (sometimes from the legal point of view) or very difficult to use. These are part of the essential process of enquiry/transaction or some other procedure within the web system. If as an individual you do not give consent to set them up, you need to stop using this particular web service. This is a case for example when you confirm you can watch a specific program on BBC iPlayer. The cookie is set to make a note of your action and to allow you to watch certain things. In Apsowebly system these cookies are usually custom, but we just introduced _gdpr cookie that is essential for the system to understand if the particular individual gave or withdrew consent to receive tracking cookies. Custom essential cookies are created on websites that use some login facilities or shopping cart procedures. As these are individual setups for some websites only, we will approach you individually and produce relevant data to display on your website in the section “types of cookies used by this website”.

Tracking cookies can be set up as third-party cookies or the first-party cookies. The most popular third-party cookies out there are Google Analytics cookies, but there are a plethora of advertising platforms or web software systems that set cookies. Apsowebly platform creates first-party cookies for your web system tracking purposes. Because of that tracking process, we need to allow users on your websites to give or withdraw consent to set these cookies. We are implementing this as the following process.

Apsowebly Cookies Privacy Policy Structures:

Type of message (loc.)	Default Message	Links Actions	Comments
Entry message – any page on your web assets left bottom corner - 300x120	This website uses cookies.	- **Explicit Consent** - **I'm ok with this** - action on this button will remove cookie message and will set full set of cookies on the machine/browser of the person giving consent - **No Consent - Cookie Settings** – link to /privacy policy page and very clearly set the bar to Block cookies - **"?"** that is going to give more info about cookies and will lead people to this same privacy-policy page that contains cookies settings. **- X** – closes message for that particular page (it will reopen message on the next page view)	The default box is designed to be mobile friendly 300x120. If you won't give consent to set cookies the message will be there throughout your browsing experience. All tracking first party cookies will expire in 24h.
Privacy Policy Page	[see new cookie-privacy policy page live]	- Easy to set/unset button for first-party tracking cookies for your visitors will be available for you the admin of the website as a tag within a WYSIWYG editor. It will be implemented on a default cookie-privacy page. Saving of that page without the default tag will create a warning message. - Various anchors within the page to allow navigation between sections of that page listing types of cookies set up on this website. Users may customise the message with links to their specific, terms of service for these parts of the system if they exist as a separate privacy-policy element. - The generic information about links to Google Analytics Settings. - Links to the popular third-party embedded content providers.	Please note - generic message is not enough and you need to make sure you customise it.
Footer message - link	Cookies Policy	The link in our opinion should be by default set in the footer of all templates on the website. This will allow users to navigate to cookies settings and manipulate cookie settings as they wish. If you are Apsowebly CMS user, you can complete this implementation in your own capacity on the majority of pages through navigation or segment modules.	Please note we cannot enforce this link to appear on your website. It is our recommendation for you to approach us about the implementation if you are stuck on a particular problem.

Please note: *It is your obligation as a data controller to make sure that the default messages suggested by us are customised for your purposes. Our obligation as a software provider is to provide a facility for you; you must provide content for your users. We will always provide you with information on the types of cookies that Absowebly software sets up but if you use third-party providers for tracking and advertising it is your responsibility to update your cookies policy page accordingly.*

The new cookie that we will set up will be called _gdpr and is going to be set only to track users behaviour concerning the tracking cookies. It is one of the essential cookies that our software will create. The default Cookie Privacy Policy page by default will contain information about the following elements:

Apsowebly First Party Cookies (General):

Status	Name	Purpose	Used For	Set for
Necessary	_gdpr	Used to process a user's choice in relation to GDPR requirements (“I'm OK” or “Block Cookies”)	GDPR cookies settings status	730 days
Important usability and experience - First Party Tracking	_ap	Unique Tracking Session ID	Built-in tracking functionality.	730 days
Important usability and experience - First Party Tracking	_v	Page Load ID.	Built-in tracking functionality.	Until you close your browser or navigate away from the website.

Comments: *If the browser sends a "Do Not Track" (DNT) header then these cookies will not be set to ensure the session is not individually tracked. Ultimately Apsowebly websites will be working the way the user has a control to override all related to Apsowebly tracking settings not only from the website level but also from the browser level. At this point browser’s settings are treated as default option for that user. Please note essential cookies will be still served.*

Only Google Analytics (GA) related cookies will be mentioned in the default section for the third-party cookies.

Status	Name	Purpose	Used For	Set for
Website Analytics - performance	_ga, _utma, _utmb, _utmc _utmz	Used to gather information in Google Analytics software about sessions on our website.	Our performance statistics data is only analysed internally and used anonymously to remarket/advertise our website(s) and to monitor service performance.	length of session to 732 days

Additional message: *You can learn more about opt-out from Google Analytics cookies on Google website*.

You may need to add to the column “Used For” more information if you analyse Google Analytics data the way that it allows you to see individual’s behaviour and link it to the activity and personal details. This may also happen if you share your GA data with a third party.

Google Analytics cookies are going to be set when a user approaches your website. There will be no attempt to stop them for many reasons:

If we would do it all the data after 25th May 2018 in the Google Analytics would be different from the data prior to 25th May. For example:

- You would not be able to see bounce rate (it would be theoretically 0%) and
- the number of users would be significantly lower

If you feel that these cookies should not be served on entry, please let us know. There are several options here including removal of GA tracking from your website. This is a valid option for certain businesses and has been already chosen among our customers.

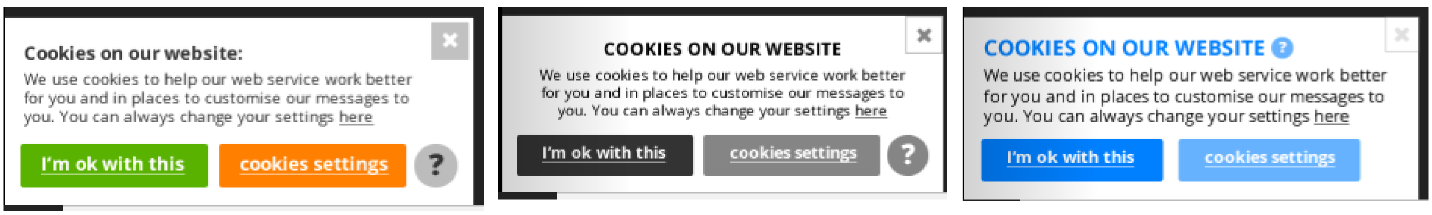
Please note: *Google Analytics as a separate data processor updates its policies and recommendations in similar to this paper communication to Google Analytic’s administrators. From 25th May they allow a new set of tools for example data retention. There are different resources on Google infrastructure related to Privacy Policies and GDPR specifically*.

By default, we also give links to Google/YouTube, LinkedIn, Vimeo, Facebook and Twitter privacy policy/cookies pages as these are the most popular embedded content providers and within Apsowebly WYSIWYG editor you can find functionality to embed YouTube content.

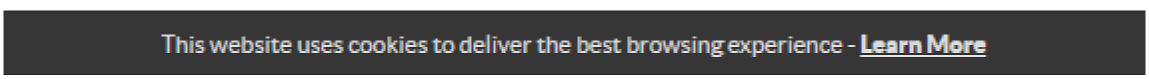
It is worth to confirm information about Adwords cookies or other third-party cookies will only be implemented on these websites which are using AdWords or other marketing services through Absowebly.

Please note: If you run Apsowebly software, and you run AdWords or other advertising and tracking within your own capacity or through the third party you need to take care of these notifications yourself. This is also valid for any other third-party cookies that your website might be using.

Some customisation of display features around privacy policies/cookies info display mechanism is possible for projects that already use some high levels of customisation, but we would appreciate if you could approach us about that when the default option becomes available as a generic mechanism within the software as described earlier.



Majority of you (our customers), however, will notice at some point in early May a mechanism implemented on your website (it will replace the previous cookie mechanism that is currently in place)



at which point, let us know if you are interested in changes (**please note** request customisation of this mechanism on your website will create additional costs). We will try to make an effort for the default message to be in line with WCAG 1.0 standard (web accessibility).

3) Collecting as little personal data as possible and consents to process it on a different level

There are two elements to this part of the legal recommendation

- you need to respect eight individuals' rights that GDPR explicitly calls
- you need to be involved in processes that now have tighter time limits and tighter requirements for data access, security and formatting.

The smaller your database is in areas related to privacy policies elements in the first place (number of columns that refer to privacy elements) the easier it is for you to perform some critical operations, now required by law, in the area of data security, manipulation and transfer.

Directly related to the data gathering that we already touched on when we mentioned cookies is in the request for consent to process data.

Please note: Consents about data processing must be, according to GDPR, separated from your main Terms and Conditions however at this same time law recognises that contractual relationship between the individual and the company requires processing of data of that individual.

According to GDPR guidelines published by ICO, consent should put individuals in control of the information stored about them by the data controller, to allow people to make a genuine choice and give them full control.

Consent requires a positive opt-in.

You cannot use:

- preexisting general message,
- ticked boxes or
- any other method of permission by default.

Explicit consent requires an unequivocal and specific statement of approval and cannot be bundled up which means for example purchase of goods in the e-shop does not mean you are automatically subscribed to the mailing list for that shop's e-marketing. This type of action now requires being split explicitly to different processes.

Data controllers must keep consent requests separate from other terms and conditions.

Apart from being specific and granular.

You also need to be able to let people withdraw consent and tell them how to do it - this has to be as transparent as possible (as easy to withdraw consent as to give one).

Because you need to now track consent status against gathered records we need to physically make sure that for each type of consent you have a separate entry in the database. You are legally obliged to keep records who, when, how, and what mentioned to customers.

Please Note: As consent should not be a precondition of service, you need to inform us if you have any additional purposes for the data obtained on your website. If this is the case the text together with the "empty tick box" will be introduced to your website. This should be the case if you gather information for marketing purposes or in case you are sharing or exporting data to third parties. You do these things when you email people some marketing information.

The regulator recognises in some areas it will be difficult to obtain consent and encourages businesses to use some other processes to allow data accumulation and verification. This part could be individual to your trades and is often specified by industry level laws and regulations.

The immediate change to the processes on Apsowebly should involve reconfiguration of existing forms and submission processes. Absowebly as a data processor is not responsible for gathering consent from the general public on your website which means all texts related to the consent and points of approval must be delivered by you - the data controller. As a web software provider and the data processor, we are introducing to the software default mechanisms and processes that will allow for implementation of your content related to the GDPR consents and privacy policy.

Some of you already contacted us with your text consent updates but if you haven't done it yet please let us know ASAP!

Of course, our software is fully customisable and allows for bespoke implementations of solutions that are relevant to your specific industry or company specific requirements. Please be aware we only deal with general rules by default. If you have special requirements and custom changes, these may create additional workload and costs and the sooner you will talk to us the better.

In some cases, placeholder text that is going to be implemented by us to hold the place for your copy on all forms is related to the default consent to process data by the first party necessary in relation to the service. This involves an introduction of some text next to the submission button (a privacy policy text link with a clear short explanation what kind of processing of data takes place). In some cases, if we believe there is not enough information about processing on our side to use our placeholder text we won't put text at all.

Please do remember facility to implement the text and the privacy policy page will exist no later than 18th May 2018 on all Apsowebly powered websites, and you are solely responsible as the domain name owner and website administrator for contacting us and triggering implementation from your end! Please remember our Terms and Conditions explicitly mention we are not responsible for the content on your website. We are web software provider, not a content provider.

Proposed Consents on General Forms (this does not apply to some hidden behind logins forms and some other processes that are non-standard processes).

Consent Type	Text Example (Important: this is an example of the possible text NOT a template! Do Not Use It)	Absowebly Action (Data Processor)	Data Controller Action (You)
General for processing data submitted in relation to the enquiry/ purchase	By submitting this form online, you allow for processing of your data by our team in relation to that enquiry. This data is not passed to third parties unless we receive further consent. - [link]full privacy policy details[/link]	Will prepare space for the text based on the number of words mentioned in "Text Example" column. Where possible this will be positioned immediately before or after your form's submit action. We will set the link to full Privacy Policy page to open in a new window. All to be tested for basic responsiveness.	You must deliver text to Absowebly for input in the forms with the view "more is less". You need to make sure your privacy policy elements follow GDPR, and you need to make them clearly available, i.e. link. If you do not deliver your text, the default text that might be wrong for your circumstances could be implemented anyway. It is necessary for you to decide how your internal processes impact privacy from GDPR perspective to communicate correctly with your web users.
For processing and passing data to third party	By submitting this form, you allow for processing of your data by our team in relation to that enquiry, this processing involves sharing some of your data (for example name and email) with other companies (our suppliers) and is necessary for the successful processing of your enquiry. - [link]full privacy policy details[/link]		
For online marketing and e-marketing with Absowebly (Sendgy)	By submitting this form, {or} By ticking the box you agree to receive our newsletters, important updates, sales and other marketing related information. Processing software complies with EU-US Privacy Shield Framework and GDPR.	Tick Box with associated text and links to the privacy policy (opening in a new window) on each form that is appointed to collect this type of data.	Provide Terms of Consent for online marketing activities. Please check if you do not process data outside of the EEA. Due to character of e-marketing our Sendgy uses in operational chain EEA and USA based providers. All are signatories of the EU-US Privacy Shield Frameworks as well as EU Model Clauses and follow GDPR requirements.
For online marketing and e-marketing with a third party	Please refer to your internal processes	We will implement your custom text on forms.	Review your suppliers if they are outside of the EU you must put information about it. Check if you do not process or export data outside of the EEA.

For processing data outside of the EEA	By submitting this form, you understand your data might be processed outside of the EEA.	Absowebly does not store or export private data outside of the EEA. Only some automated processes related to sending marketing emails take place outside of the EEA (Sendgy).	Provide an exact text for the consent related to data export outside of the EU if you use some other software or the third-party providers.

Please Note: All of you who are data controllers are responsible for your texts and communication processes on your website.

An extended option will be available for those who run online and email marketing through Absowebly. If you run e-marketing with Absowebly, we will approach you about explicit consent mechanisms for Sendgy.

If you are running an email marketing through the third party, you need to approach us with the full required text ready for implementation.

Please note: When you cancel your services with us or your current supplier your circumstances may change, and you need to review all related to GDPR consent texts!

4) Right to be forgotten - right to be erased

Article 17 Right to erasure (‘right to be forgotten’) of Section 3 in Chapter III of the GDPR mentions extended to the previous right to be forgotten elements.

This creates a direct impact on any software processes, and we established the following structures to deal with these requests:

- Although GDPR only specifies processing as "without undue delay" ICO tells us to process it on a controller's side with no longer than a month. For our technical purposes, we need to reserve two weeks (14 days) from the moment you send a written request to support@absowebly.com to erase particular user records to the moment we can confirm that technically particular user has been forgotten/ anonymised. If within 48h (working days Mon-Fri) you do not have a clear reply from Absowebly team member that this request is acknowledged and we are working on it, please make sure you contact us again (unfortunately emails are not 100% reliable forms of communication).

- Interestingly it is worth to remember “Right to be forgotten” is not an absolute right. The simple reason for why it is not is that you may have some other legislative obligations to keep data on record (financial or criminal records that have independent timescales for expiry). The paradox of the law is that you need to be able for to identify somehow users that asked to be forgotten (keep some sort of record of these requests).

The original right to be forgotten is now extended. This is partially the reason for the introduction of the alternative name "right to erasure" that now also puts the responsibility on data controller to pass information about removal of the data from the other databases (your cooperating companies – other data controllers).

The basic example of why this cannot be an unconditional right could be that person who bought goods from your company then asks to be forgotten before you are able to process their order which creates a situation that you are unable to do anything with the order (not even to return the money).

Interpretation of this types of situations is not a subject of this support article, but it does create a lot of question marks for the future. Perhaps these interpretations will be made available when real cases will be introduced to the life. In the current situation, all we can do is to stick to the given rules as much as possible, follow official guidelines and make sure we use common sense to process our data and use the strictest possible processes to keep databases in the correct order. With this right in place, we will introduce one more limitation that is very much related to the data ageing and right to be forgotten.

From 25th May 2018 you will be only able to get from us backups of your data that are up to 372 days old, opposite to requests that you could place up to now. This will limit your access to old data with records that were subjects to “right to be forgotten” enquiry. This way we will have two processes in place.

- Immediate removal/anonymisation - the live database actioned within 14 days from the request coming through to Absowebly.
- Automated removal from any backups after 372 days (this is only emergency data, and you do not have access to this data. In case this data needs to be activated for you to view we will scan it against existing “right to be forgotten” records

Please note we will need to remove at this stage information about a person that creates a set of obvious identifiers, but we are not going to remove the record from the database as this may affect reporting and database structures the way that they become impossible to use. We will remove content from all affected fields and replace it with some indicator of “GDPR Right to be forgotten request” we will keep a record of the request for the removal (date and some unique identifiers – email address, name). As these types of requests are a new element of the regulation, we expect to establish some routine processes when these are coming through. Please note that based on a volume of these requests we may decide to adjust our terms and conditions in the future to make sure these requests are formalised within our services.

5) Security by design

Keeping minimum data in the system is our first and basic step towards data security through Apsowebly design. Of course, we use further mechanisms to make sure we make sensitive data very difficult to obtain from the software layer.

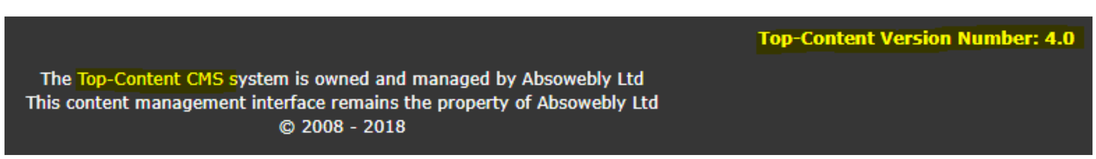
Unfortunately, as we all know, the problem with data and systems security is that all the systems are only as secure as a password that protects them. Often it is not the password security and complication itself, but the way it is stored, that creates security issues (text file “passwords” on your desktop or little sticky note on the monitor).

Technology gives us now more opportunities to implement crucial changes to the web systems. Elements that we improve, and we will be improving over the next 12 months are not all directly related to the GDPR, but they will all contribute to the increase of “security by design.”

Top-Content and Security by design

The changes in the general arena of web security, as well as legislation, are the main reason why in 2018 we have to withdraw the support for our first software platform Top-Content that we stopped developing in early 2015. The final version T-C v4.5 was a comprehensive CMS system. But due to changes in technology, we decided to build a development platform Apsowebly on the top of which we used elements of Top-Content within Apsowebly’s CMS module. Some of our clients still run different versions of that software on their websites, and over the coming weeks and months, we are replacing the last remaining websites that are running this software with a new installation of Apsowebly platform.

Please Note: It is likely that you are a Top-Content user if your website development started



before March 2015. If you want to check it now go to {your domain}/admin and look at the interface if the page you will see has a clear reference to Top-Content you are scheduled for a shift to the new Apsowebly platform. You do not need to do anything as we will notify you about changes when necessary.

Beyond GDPR

For 10 years our software creates a secure business environment for business data processing. We are part of the very dynamic web industry. New technologies that deal with security and processing of data emerge daily. As these solutions become operational and commercially viable, we are looking to improvements in database management which may lead to the new security by design processes to be implemented.

In the long term, these processes are not GDPR related, but they are implemented as they help to enhance your data and our software security. It is important to remember that sometimes with security comes restriction to usability.

Apsowebly always uses structures around payments that comply with PCI DSS SAQ-A or A-EP to allow the process to be outsourced to PCI DSS compliant 3rd parties. This eliminates the most sensitive data from the database.

The weakness of the Password mechanisms creates the opportunity for us to explore and implement 2-step or two-factor verification process within Apsowebly for users' login. To decrease chances for password related issues, we will implement within the next 10 months system of verification that is going to use emails, SMS or other processes.

This part of the security system with auto logout based on time and hardware/software configuration is going to bring Apsowebly User login to the top-end technology giving our software full marks in the area of "security by design".

For GDPR

In the short term (by 25th May 2018) there are several updates in the area of security by design that we are going to implement.

During the next few weeks, we will introduce some data scrambling on the Apsowebly platform level. This introduction is going to create some restrictions on database search. To follow GDPR recommendations, we will scramble data in some columns that are currently searchable. The most impactful elements will be in the area of address fields as not all of them will be possible to search. Columns with some additional personal information will also be obstructed. We will introduce this element individually to project managers, and although there will be some adjustment needed on your end, we will try to keep disruptions to a minimum.

We are also opening an alert service that we hope never to use it - we never had to (touch wood).

This is Security Breach Alert. In case of security breach, Absowebly will inform you (the data controller) within maximum 72 hours of any detected breaches that involve possible privacy data protection elements. We have monitoring in place since we develop software. Although we were in the past under different attacks (from attempts to place malware on our infrastructure through SQL injections to cross-site scripting and all sorts and versions of DoS), we had no problems on the software layer, and we managed to stop all attempts (touch wood again). The only time when something bad happened was when passwords on the clients' side were compromised.

Over the years we implemented some restrictions in the software that limit chances of the regular attacks. Combined with the user management in Apsowebly we are likely to limit at this stage a lot of attempts "by design". With GDPR coming to life we need to produce a clear system for communication "just in case" to give you all an opportunity to create full structures of crisis management on your side in case of any successful breaches. This is covered by our new service. In case of the breach you will receive the following information:

1) The time of the successful attempt

2) The description of the type of problem that was detected
3) What kind of data is understood to be compromised
4) Who are the perpetrators (as much data as possible – although please remember it might be very difficult to obtain that data)

It is worth to mention that as a part of the security by design process we select our suppliers very carefully. All of them use reputable and secure infrastructure with processes and accreditations complying to voluntary schemes like EU-US Privacy Shield Frameworks, ISO 27001:2013 (Information Security) etc. The GDPR applies to all organisations all over the world as long as they process data of individuals from the EU/EEA. GDPR does not restrict the use of web services from the outside of the EU but to make it very clear all Apsowebly data processing is taking place within EEA infrastructure on the software that has been developed within EEA by EEA based company.

In relation to our project we use the following suppliers

- Hosting Companies / Cloud Services - for example: OVH, Black Night, Rackspace, Memset
- Domain name registration companies - for example Webfusion, eNom
- Email marketing processing - for example: Rackspace Cloud, Amazon Web Services
- Transactional Emails Processing Services – for example: Google G-Suite, Amazon Web Services
- Address Search – for example PCA predict, Logate

Summary with schedules

To keep it simple, see a summary of actions taken by Absowebly in response to GDPR full implementation:

1) Apsowebly software uses now simplified cookies structure including new _gdpr cookie to store preferences regarding cookies consent. Some changes in this area are already online, and all will be active by 25th May 2018
2) The Apsowebly default web cookies privacy policy page is updated, please check the draft version here
These changes will be implemented by 25th May 2018. This page will, by default, allow people to withdraw their consent regarding tracking cookies settings.
3) For standard users Apsowebly default cookie message compliant with GDPR will be available online on your websites by 18th May 2018 – you will be able to customise it if you like.
4) If you want to customise the appearance of the default Apsowebly cookie message, please talk to us when you receive communication from us. All communication on that side should not start until we approach you or after 25th May 2018 when all necessary processes are online. Please concentrate on the legal aspect of your message that is crucial before you switch to the appearance of your message.
5) We have 72h from the detection of the breach that can affect data related to privacy policies to communicate full report about the breach to you, the data controller in order to let you make decisions on your end.
6) We Reserve 14 days out of regulators 28 days to process “right to be forgotten” requests.
7) From 25th May 2018 backups will be only available for a maximum of 372 days
8) Absowebly software does not store very sensitive data like credit cards numbers.
9) Absowebly should not be used for processing of PAYE; it is not a tax processing software.

You the Data Controller are responsible for the entire data stored within your installation of Apsowebly system. As a data processor, we have limited control over the data that is inserted into the system. We do not monitor individual entries, and we only act on records within your data if there is a specific/explicit request to do so coming from you or your team member.

If you have any questions around GDPR, please let us know.

Team@Absowebly