

GDPR in the recruitment sector. A complete overview



TABLE OF CONTENTS

03 - The GDPR in the recruitment sector. A complete overview

04 - The Processor Agreement

07 - Consent in the recruitment sector

15 - Retaining and retention periods

20 - The current database

23 - Only necessary data

26 - Information obligation

33 - Documentation obligation

36 - Accountability

38 - Right of access

41 - Other privacy-related matters

43 - Afterword OTYS

46 - Processes OTYS



The GDPR in the recruitment sector. A complete overview

The document in front of you is as complete as possible in respect of the consequences the GDPR (General Data Protection Regulation) may have for you. This applies to all our customers: from secondment, recruitment & selection and/or temporary employment agencies to, most definitely, all corporate recruiters and job boards. The main purpose of this document is to answer as many of your questions as possible.

This white paper also provides answers to questions such as:

- ▶ What should I do with my current database?
- ▶ Can I still source?
- ▶ Do I have to conclude a processor agreement?
- ▶ How does OTYS deal with retention periods?
- ▶ Can I automatically set processes?
- ▶ What are laws and what are guidelines?
- ▶ Do I have to delete candidates or can I also anonymise?
- ▶ Which objectives must I meet in the recruitment sector to be compliant?

OTYS has prepared this document on the basis of questions you asked during the webinar of the 29th of last November.

We hope to fully answer your questions in this document. If you have any other questions, you can always contact OTYS or Lora Mourcous of Solv via mourcous@solv.nl.

If you have any questions that are not answered in this document but pertain to OTYS, please contact your account manager or, in the event of a general subject, marketing@otys.nl. We are happy to help.



The Processor Agreement



The Processor Agreement

Who is the processor?

The GDPR, effective per 25 May 2018, will replace the Dutch Personal Data Protection Act (DPPDA). The GDPR uses the terms 'controller' and 'processor' that were also used in the DPPDA. In the GDPR the following definitions are of interest:

Controller: *a natural or legal person, a government agency, a service or any other body that, individually or jointly with others, determines the purpose and means of the processing of personal data; (in this: the OTYS customer).*

Processor: *a natural or legal person, a government agency, a service or any other body that processes personal data on behalf of the controller (in this: OTYS).*

As a mediation agency or corporate recruiter you are regarded as a 'controller' because you make use of the OTYS system to store and process the personal data collected by you. OTYS itself is the 'processor' in this relationship and facilitates functionalities to comply with the GDPR. Do note that OTYS facilitates and advises, but that you, as agency, are responsible for the actual execution and settings that pertain to the GDPR.

OTYS as processor

In this situation OTYS is the processor who is obliged to draw up a processor agreement for all its customers. All customers will find this agreement in their mailbox before the end of this year. It is essential to sign and return this agreement before 25 May, 2018.

The OTYS customer and the Processor Agreement

Our customers do not have to present their candidates with processor agreements (only laws and guidelines with regard to consent and retention periods apply to candidates, see chapters 'Consent in the recruitment sector' and 'Retaining and retention periods'). However, it is mandatory to conclude a processor agreement with all data processors that you engage with as a company (e.g. payroll companies, back-office parties, etc.). If a supplier fails to present an agreement, the OTYS Processor Agreement could provide a good basis for this. When adapting the agreement, make sure the changes are checked by a lawyer.

During and after the webinar of 29 November, we received questions about the conclusion of processor agreements with candidates, prospects and clients/customers. No processor agreements have to be concluded with these groups, the major reason being that there is no processor in this situation (neither of the parties is a processor). For answers as to what you should do with these groups, we refer to 'Consent in the recruitment sector' in this document. What you do need in order to approach these parties, is their consent.

OTYS and its suppliers

OTYS enters into processor agreements with its suppliers. Our customers do not have to enter into agreements with the suppliers (e.g. data centres) of OTYS. Such constructions are not desirable.

Consent in the recruitment sector



Consent in the recruitment sector

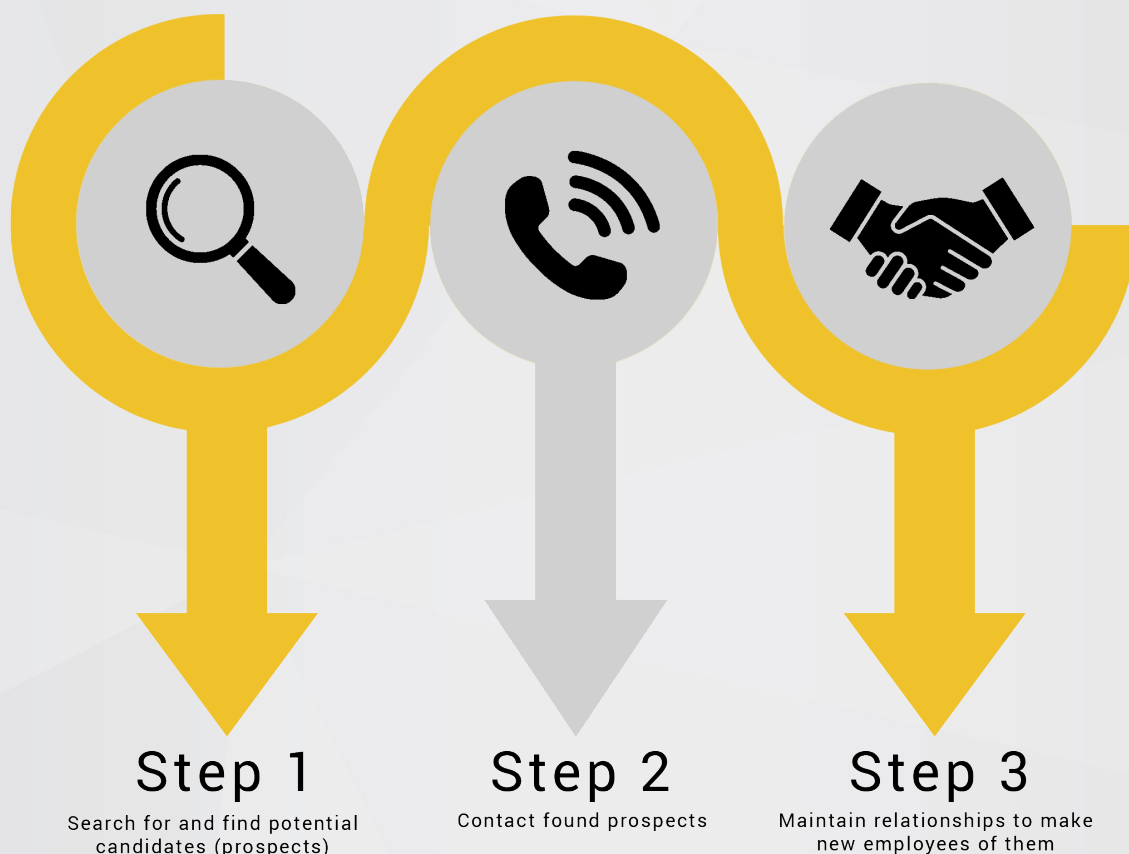
Can I still approach candidates without consent?

As is currently the case, you can also call a person or organisation or send mail with an offer without the receiving party's consent under the GDPR. However, if you send an offer via a digital channel, such as email, fax or SMS, you do need their consent in advance.

Sourcing

Many of our customers use sourcing to find new candidates for the vacancies they offer. Under the GDPR this is still possible. There are, however, a few points to consider.

There are 3 steps when it comes to sourcing candidates:



If you are currently approaching only relevant candidates through relevant, individual messages you are most probably already working in line with the GDPR. There are, however, a few matters to investigate. How can you legitimately retain this data? And how do you obtain consent to retain the data of a prospect?

Below is an example of a compliant process. This is based on the legitimate interest (see the next page for an explanation):



Screening social media on the basis of a 'legitimate interest'

If you search or source a lot via websites that are often frequented by candidates looking for new jobs, such as job boards or social profiles, or if the recruitment organisation acquires a list of contacts from a recognised source and has verified that the persons are interested, a 'legitimate interest' can be claimed. It is, of course, important to check that you do not contact candidates whose personal data you've obtained within a context from which it would appear that they never expected anybody to contact them in the first place. In other words, you have to balance the legitimate interest against the privacy interest of the person concerned.

You can also process someone's data without consent if you can demonstrate through a clear weighing of interests that this is justified and that you have taken the privacy of the relevant person into account for as far as possible. In other words: answer the question "Why does your recruitment interest weigh more heavily than the privacy interests of contacts?". You need to describe this interest in the data register, which you must be able to present to the Dutch Data Protection Authority (DDPA) at any time. For more information about data registers, see chapter 'Documentation obligation'.

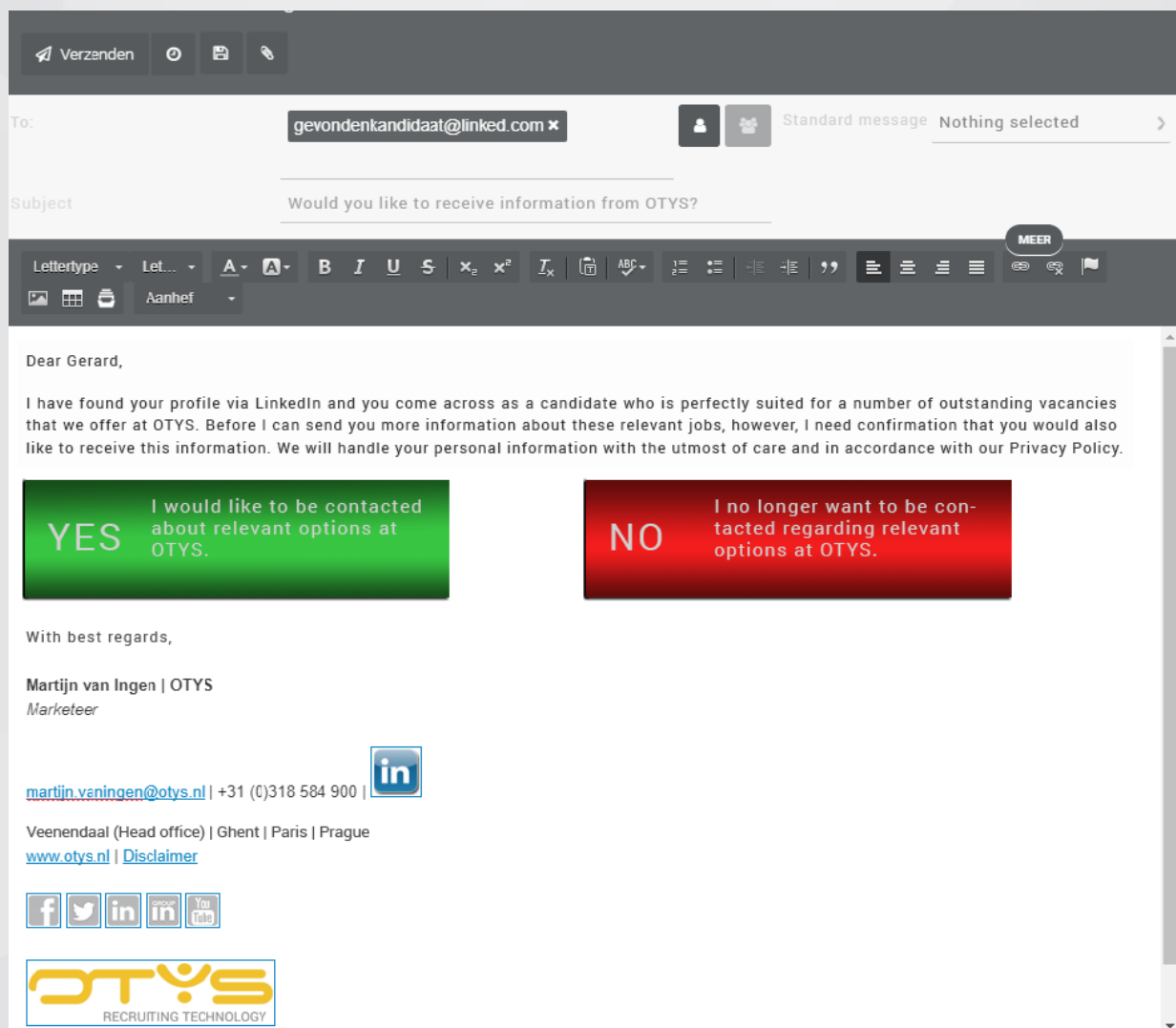
LinkedIn plug-in in OTYS

Many of our customers use it: the LinkedIn plug-in in Google Chrome that allows data from LinkedIn profiles to appear in OTYS at the touch of a button. This plug-in can still be used. However, you must still request consent in order to send any relevant information.

OTYS deals with this as follows

The moment our customer uses the LinkedIn plug-in, a new candidate will be created in OTYS. In the created candidate details a button will appear that must be clicked to

- by means of an already composed email that can be adapted to your personal wishes
- ask this person for their consent to be included in the database (retention period 12 months).



The screenshot shows an email composition interface. At the top, there's a 'Verzenden' button and icons for attachments and links. The 'To:' field contains 'gevondenkandidaat@linked.com'. The 'Subject' field contains 'Would you like to receive information from OTYS?'. Below the subject field is a rich text editor with various formatting options. The email body starts with 'Dear Gerard,' followed by a paragraph explaining the purpose of the email and requesting consent. Below this text are two large buttons: a green 'YES' button with the text 'I would like to be contacted about relevant options at OTYS.' and a red 'NO' button with the text 'I no longer want to be contacted regarding relevant options at OTYS.' The email concludes with 'With best regards,' and the signature 'Martijn van Ingen | OTYS Marketeer'. Below the signature is a LinkedIn icon and contact information: 'martijn.vaningen@otys.nl | +31 (0)318 584 900 |'. Further down, it lists office locations: 'Veenendaal (Head office) | Ghent | Paris | Prague' and provides links to 'www.otys.nl' and a 'Disclaimer'. At the bottom, there are social media icons for Facebook, Twitter, LinkedIn, and YouTube, and the OTYS logo with the tagline 'RECRUITING TECHNOLOGY'.

Verzenden

To: **gevondenkandidaat@linked.com**

Standard message Nothing selected

Subject: **Would you like to receive information from OTYS?**

Lettertype Let... A A B I U S x₂ x² I_x ABC

Aanhef

MEER

Dear Gerard,


I have found your profile via LinkedIn and you come across as a candidate who is perfectly suited for a number of outstanding vacancies that we offer at OTYS. Before I can send you more information about these relevant jobs, however, I need confirmation that you would also like to receive this information. We will handle your personal information with the utmost of care and in accordance with our Privacy Policy.

YES I would like to be contacted about relevant options at OTYS.






NO I no longer want to be contacted regarding relevant options at OTYS.

With best regards,

Martijn van Ingen | OTYS
Marketeer

martijn.vaningen@otys.nl | +31 (0)318 584 900 | 

Veenendaal (Head office) | Ghent | Paris | Prague
www.otys.nl | [Disclaimer](#)

OTYS
RECRUITING TECHNOLOGY

Requesting consent is a requirement under the GDPR. Unless you send a personal message via LinkedIn. In that case you will not include this person in your database. If you want to include this person at a later stage, you will have to ask for their consent in accordance with the above process.

If the candidate clicks on 'yes', they will be included in the database resulting in the following automated (manual also possible) process running in OTYS: after 12 months this person will receive a reminder to update their profile and to give their consent to extend their profile for another 12 months.

A person may be included in the database without consent (for a maximum of 30 days according to the GDPR regulation) when it can be demonstrated that consent has been requested in the meantime. If the candidate does not respond to this, our customers could opt for setting up a standard reminder. OTYS will set this at 7 days by default and this timeline can be adjusted by our customers. If there is no response from the person concerned, the consultant will be notified after 2 weeks (can be set individually) that the data of the person concerned will be anonymised. This anonymisation action cannot be reversed.

The complete deletion of candidates will remain a manual process.

Automatic updating

One also needs to obtain consent for the automatic updating of candidate profiles by the LinkedIn plug-in. This question can be asked in the proposed email, for example. OTYS includes this question by default.

Candidates

Candidates who apply for a vacancy must be given the opportunity to give their consent for being included in a database. This can be done by placing a check mark in a box that has not been pre-checked. If candidate data is included in a database, this category (candidates) must be described in the data register. For guidelines on how to proceed, see chapter 'Documentation obligation'. For guidelines on retention periods, we refer to chapter 'Retaining and retention periods'.

On the platform, OTYS has provided the technical solution that enables the giving of consent by means of such check marks. A note here is that these will not be 'on' by default. We will inform all our customers clearly on how this can be set.

To save and process personal candidate data you, as controller (the OTYS customer), require the candidate's consent. No processor agreement is needed for this candidate as there is no processor involved in this relationship (candidate-agency).

Prospects

Offering one CV to a prospect (organisation) is still legitimate under the GDPR. Once it's done in bulk (i.e. an email to the database) the same applies as for the candidates; all separate contacts must have given their consent to be approached for this purpose, it must be named in the data register and guidelines apply regarding retention periods. The same automated process that applies to the above candidate module will also be implemented in the relationship module.

Newsletters

In the field of email marketing, there are not many changes in comparison to the DPDPA. You may only email persons who have given their consent (an opt-in) for receiving your mailings or newsletters. This opt-in must be filled in voluntarily and not pre-checked by default. An opt-in may never be part of the general terms and conditions and the recipient must be informed as to what the data will be used for. For every set purpose, sharing this data with other parties in addition to processing this data, for instance, you must provide the option of placing a check mark. These options are already possible in OTYS and need only be organised as preferred. You will find several examples of texts in this document. When creating new interaction forms, you should consider the following:

- ▶ The information that is necessary;
- ▶ Indicate retention periods;
- ▶ Request consent via a not yet entered check mark;
- ▶ Refer to privacy statement.

The already existing opt-out will continue to exist as the option to deregister remains part of the GDPR.

Retaining and retention periods



Retaining and retention periods

How long can I retain the data of my candidates and contacts?

Where the GDPR is concerned, it doesn't matter whether you are employed in recruitment & selection, secondment or in a sector outside the recruitment of personnel. As soon as you are processing personal data, the GDPR applies to your organisation and so do the associated retention periods. In respect of the exact retention periods, this regulation is not that specific. The GDPR provides the following description of the retention period:

"Personal data shall no longer be retained in a form that allows identification of the data subject than is necessary for the realisation of the purposes for which they are collected or subsequently processed."

Retention periods, legal or guideline?

It must be clear in advance which data you collect and what the purpose is for processing the data. On this basis the data may not be kept longer than necessary. You must be able to give the Dutch Data Protection Authority a thorough substantiation of your data processing if they ask for it. There are, however, specific laws that can prescribe a retention period. The most important in respect of recruitment are:

Legal:

- ▶ Data from the payroll administration that is important for tax purposes: 7 years (post-employment employee)
- ▶ Statements of taxes on wages: 5 years (post-employment employee)
- ▶ Copy of proof of identity: 5 years (post-employment employee)

Guideline:

- ▶ Personnel file: Guideline; 2 years (post-employment employee, unless you no longer need it within 2 years)
- ▶ Job application details: Guideline; 4 weeks after the conclusion of the application procedure (if the job is not assigned)
- ▶ Job application details: 1 year with the consent of the applicant (if, for example, a suitable job becomes available at a later date).
- ▶ Ex-customers: As soon as the 'customer relationship' is over. There is no fixed period for the customer relationship but it should be more or less in line with the duration of the average agreement or slightly longer. From this perspective a period of 2 years can be easily substantiated.
- ▶ 'Marketing contacts'; no longer than necessary, indicate accountability in the data register.

Anonymise and pseudonymise data

It is not always immediately necessary to delete data from your database. You can also choose to anonymise or pseudonymise this data. If personal data is anonymised, it is no longer possible to determine the person this data originated from. However, you can see trends and use the data for preparing reports. When the data is completely anonymised, the GDPR no longer applies. For the very simple reason that it no longer refers to personal data.

However, the GDPR does apply if personal data was pseudonymised. With pseudonymisation, personal data is processed in such a way that it can no longer be directly traced back to a specific person. Here, the identifiable elements of this data are removed. For example, the name is deleted or the complete data set is re-encoded into a number. The requirement for pseudonymisation is that the source data is still present. Once this data is deleted, or re-identification is otherwise impossible, it is referred to as anonymous data. The GDPR, therefore, applies if personal data is pseudonymised which makes the previously mentioned retention period also applicable.

As indicated in the chapter 'Retaining and retention periods', OTYS will proceed to anonymise the data by default. This is an automated process linked to a so-called 'Due date'. A candidate is assigned this date as soon as they appear in the database. With each action of the contact person the Due date is postponed. After having given their consent for inclusion in the database, for example (Due date is extended by 12

months). When data must be deleted on the basis of the Due date, 4 weeks after completion of the job interview and when no permission is given for inclusion in the database, for example, the data will automatically be anonymised. The complete deletion of persons remains a manual process.

Consent and retention

You may retain the details of a candidate in your file for longer, provided that they have given their consent for this. As the GDPR doesn't impose strict periods, it is also possible to retain data for longer than a year. This is perfectly conceivable if your database contains self-employed persons without staff, freelancers or persons who have explicitly indicated to only be available again after a long period of time. So make sure to always properly document this so that you can easily justify it to the Dutch Data Protection Authority! What is important to know is that the GDPR applies to all new personal data in your database. The rules that apply to your current database are explained in chapter 'The current database'. Please note: all categories of personal data (candidates, prospects, staff, etc.) must be listed in your data register. This also includes the personal data that you - for whatever reason - wish to retain for longer (for more information see chapter 'Documentation obligation').

Longer than 1 year?

If a candidate indicates that they want to be kept on file for a longer period of time, they must confirm this in writing so that you can demonstrate their consent. In your own data register, indicate the retention period of this category of candidates and why. The 12 months indicated by the Dutch Data Protection Authority serve as a guideline as opposed to a law. If business interests outweigh the privacy interest ('Consent in the recruitment sector') and if this is clearly indicated in the data register, you can still comply with the GDPR (legitimate interest).

Responsibility?

The GDPR is a uniform regulation that applies to everyone who processes personal data in any member state of the European Union. Everyone must, therefore, act according to the same points of departure and be able to substantiate their actions responsibly. The fact remains that each company is responsible for its own actions. Here, OTYS is a processor and not a controller which means that our customers are responsible for deleting or not deleting personal data. OTYS must facilitate the possibility to do this on our platform.

Retention periods for everyone?

If you process personal data you are subject to the GDPR, regardless of whether you are an intermediary and not a legal employer. Here the aforementioned retention periods apply.

How does OTYS deal with retention periods?

OTYS offers a number of settings within our software to meet the retention period and anonymisation of personal data requirements. Options are:

- ▶ The manual deletion of files;
- ▶ Automatic anonymisation of personal data on the basis of 'Due dates'.

We leave it up to our customers to indicate their preference. The same applies to the retention periods. We can set it as such that added candidates will receive an email after 4 weeks (guideline retention period and rejection after the completion of the application procedure) to inquire whether they wish to remain in the database for another 12 months. In addition, the question as to whether this candidate wishes to be contacted in the event of relevant vacancies could also be asked. These 4 weeks can be set. However, you may want to know this at an earlier or later stage. There could be another (legitimate) reason why you would want to keep this person in your database for longer. This is why we leave the choice up to our customers. We do, however, offer a GDPR-proof setup.

The current database



The current database

What must I do to make my organisation comply with the new legislation?

Under the DPDPA you were already obliged to ask the persons you wanted to include in your database for their consent. Where your existing recruitment data is concerned; you do not have to delete this data, provided it was legitimately obtained. This means that you must have the explicit consent of these persons to be listed in your database. In addition, you also have to take into account that you can only use the data for the original purpose. If a person has applied for a specific vacancy, you are now no longer allowed to speak to them about other vacancies without their consent.

What should you do?

Very simple; you must ask your candidates to agree with future communication. That is, if you want to keep these persons in your database.

Those who have already given their consent to be contacted about that one particular vacancy, for example, can still be kept up to date on that vacancy. If you decide to send these persons other information, you will first have to obtain their consent for this.

What is OTYS' view on this?

We want to facilitate our customers in keeping the database up-to-date in order to comply with laws and regulations. This means that we will help our customers achieve this. **We will offer an automated solution where you can indicate whether you need it or not.**

The solution will immediately request an update from all data subjects in the current database in order to give their consent to be included in the database for longer.

If there are currently contacts in your Candidates or Relationships database for which you cannot present their consent should the Dutch Data Protection Authority come knocking on your door, it would be wise to ask these contacts for an update before 25 May 2018.

Consent?

If your contacts give their consent to keep them on file for 12 months they can remain in your database. OTYS will then automatically send the same consent email after 12 months so that these contacts can choose to remain in your database for another year.



No consent?

OTYS can anonymise data. Profiles and files can be completely deleted manually, but you can also opt for running a script that will automatically anonymise the personal data. The latter option is standard in OTYS because in this way you can - continue to - benchmark. Results achieved in the past will continue to exist and can be used as a basis. Based on this data, the reporting module in OTYS will show correct comparisons and results. And, last but not least, by anonymising data of persons who no longer wish to remain in your database, you will comply with laws and regulations.

*OTYS will keep its customers informed of this solution.
For a clear diagram of this process, see chapter
'Processes OTYS'.*

Only necessary data



Only necessary data

What can I ask for and what am I not allowed to ask?

The GDPR prescribes that you request the least possible personal data from your contact person. This means that if you only need an email address, you may not ask for their address and telephone number. There are, of course, situations to be imagined in which requesting an email address seems not entirely necessary. See the following question from one of our customers:

"Publishing a white paper usually has a lead-generating character. To provide the white paper one would need, in fact, only one email address (maximum). Does this mean that you are not allowed to ask for more information than merely the email address? (Such as the name of the person, telephone number, ...) In fact, if you can simply download the white paper, you don't even have to ask for an email address. How does this work under the new regulation?"

If you inform these persons of the purpose for which their data will be stored (information obligation), and if they give their consent for this and you adhere to the retention periods and documentation obligation, there is no reason not to ask for an email address. Although the GDPR gives the 'power' back to the consumer, they can still be approached if they give their consent for this! However, where the downloading of a white paper is concerned, the phone number and home address are not relevant, so you cannot ask for it. It may be that by asking for an email address you make the threshold for your downloads too high (they don't want to give their consent to stay in a database for longer). You could keep an eye on this yourself and then perhaps make sure that you start binding people to you in a different way (e.g. inbound marketing).

Interaction forms

Interaction forms can be created in OTYS in various ways. This is something our customers can decide on for themselves. We can, therefore, only indicate that attention must be paid to the amount of data requested - just ask for the most urgent data.

Purpose of processing

What OTYS facilitates is a possibility to broaden/specify the purpose of saving data. For this, the following option can be added to interaction forms on your own (OTYS) website.

Below is an example of what that might look like.

Are you interested in receiving more news from OTYS?*



OTYS news / updates



Product releases / updates



Event notifications



Customer highlighted



OTYS advantages



Other



None of the above

Become a member of the OTYS Community

*By becoming a member of the OTYS Community you are not applying for a job, but you are giving your consent to receive newsletters and promotional statements from OTYS via email, telephone or SMS regarding news, events, product releases and updates, customer stories and vacancies at OTYS. By using this service, you agree that we will process your data and that we may place cookies on your devices.

You have given your consent to receive information from OTYS via email and/or another channel such as SMS and social media. Your personal information remains strictly confidential. You can unsubscribe at any time. Costs for notification and data may apply. Consent in respect of these conditions is not part of working at OTYS.

Information obligation



Information obligation

Which texts show my compliance with the information obligation?

The controller is subject to an information obligation. This entails, for instance, that you inform the candidates who register quite clearly about the purpose and for how long you will retain their data. You could do this by adding texts to where check marks can be placed. Below is an example:

<Company name>, as the responsible party in the sense of the Dutch Personal Data Protection Act, collects the personal data provided by you and uses this data to process your application and help you get in touch with (potential) vacancy holders, within <Company name>, so that you can be linked to one or more vacancies. We will retain your data in our database for four weeks after the completion of the application procedure. Only after you have given us your consent, will we retain your data up to one year after the completion of your application procedure.

<Company name> would like to keep you informed of news and tips. If you give your consent for this, we will send you a newsletter once a month after the application procedure has come to an end.

You can request <Company name> at any time to delete your data or withdraw your consent. More information on the processing of your personal data and rights can be found in the Privacy Statement for Applicants of <Name company> [\[hyperlink\]](#).

I give <Company name> my consent to retain my data in the database for one year after the completion of the application period so that I can be linked to one or more vacancies and <Company name> can contact me in this regard.

I give <Company name> my consent to use my email address so that <Company name> can contact me to share news and tips.

How does this work in OTYS?

The above functionality is technically supported by OTYS. One could also choose to anonymise the data after the retention period of 4 weeks or 1 year (for this see chapter .. "Retention period"). OTYS offers a standard text which you can customise. When doing so, keep the following in mind:

- ▶ Do not ask for unnecessary data.
- ▶ How long do I retain the data?
- ▶ For what purpose?
- ▶ Do I use clear language to describe this?

Privacy Statement

The privacy statement must fully include how your organisation deals with personal data. The privacy statement could be a page on your site that (briefly) shows what this white paper is about. It is an informative message to your customers or candidates about the processing of personal data. On the basis of the privacy statement, the customer or candidate can decide whether or not to enter into an agreement with your organisation or make use of your services.

The GDPR does not prescribe a mandatory format for a privacy statement. However, it is advised to minimally state the following:

- ▶ The identity of the responsible person;
- ▶ The identity of the Data Protection Officer (if applicable);
- ▶ The contact;
- ▶ The data processing purposes and whether this data is distributed outside the EU;
- ▶ Retention periods;
- ▶ To what extent it is mandatory to provide data;
- ▶ Who the recipients of the data are;
- ▶ If use is made of automated data collection;
- ▶ The rights of the parties involved;
- ▶ The security level;
- ▶ Whether the provision of personal data is a legal or contractual obligation or a necessary condition for concluding an agreement, and whether the data subject is obliged to provide the personal data and what the possible consequences are when this information is not provided.

According to the GDPR, the above information must be easily accessible and comprehensible, and that the language used is clear and simple. The amount of information to be provided and the criteria that said information must meet are quite different in comparison to the DPDPA. Many organisations will have to amend their privacy statements and this is very important. If the company does not have a (complete) privacy statement they will be fined a maximum penalty of EUR 20,000,000 or 4% of the worldwide turnover (if the latter is higher) once the new GDPR has come into effect.

Do you want to immediately see an example of a well set up Privacy Statement? Check the below websites:

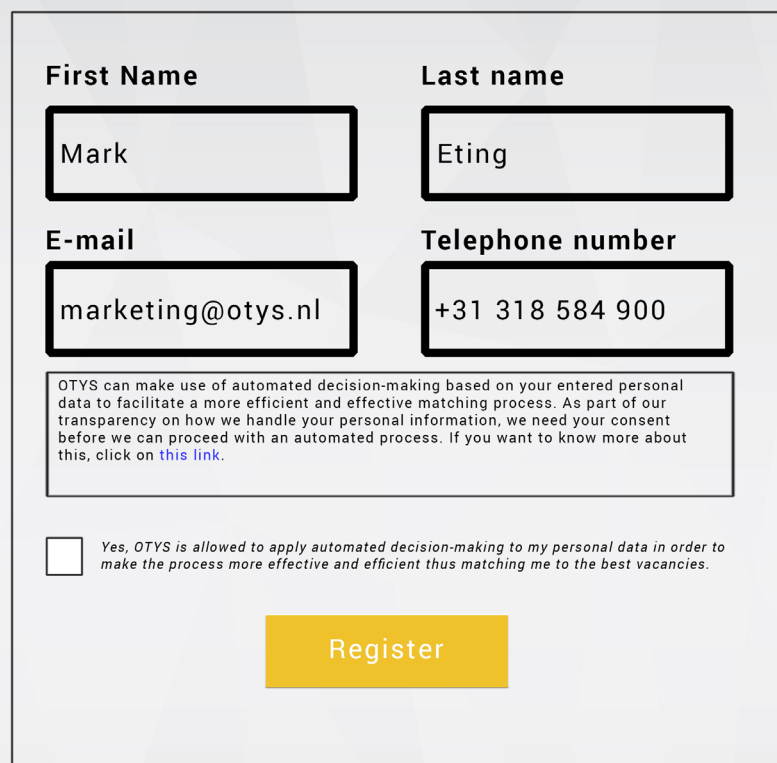
www.solv.nl/privacy/62

[www. autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/privacystatement-autoriteit-persoonsgegevens](http://www.autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/privacystatement-autoriteit-persoonsgegevens)

Automated decision-making

Automated decision-making (think of the OTYS killer questions) is not prohibited. It is, however, mandatory to indicate to a candidate that use is made of automated decision-making.

This can be done by adding this text at the bottom of a consent form, for example, as can be seen on the next page.



A registration form for OTYS. It contains four input fields: 'First Name' with the value 'Mark', 'Last name' with the value 'Eting', 'E-mail' with the value 'marketing@otys.nl', and 'Telephone number' with the value '+31 318 584 900'. Below these fields is a text box containing a privacy notice about automated decision-making. At the bottom is a checkbox for consent and a yellow 'Register' button.

First Name	Last name
Mark	Eting
E-mail	Telephone number
marketing@otys.nl	+31 318 584 900

OTYS can make use of automated decision-making based on your entered personal data to facilitate a more efficient and effective matching process. As part of our transparency on how we handle your personal information, we need your consent before we can proceed with an automated process. If you want to know more about this, click on [this link](#).

☐ Yes, OTYS is allowed to apply automated decision-making to my personal data in order to make the process more effective and efficient thus matching me to the best vacancies.

Register

Cookie Policy

Cookie legislation will change in 2018 thanks to the GDPR. Per 25 May 2018, the European Commission demands (e-privacy regulation) that internet users can accept or refuse privacy-sensitive cookies via their browser settings. In the current Dutch cookie legislation permission is requested per website. In many cases permission is required to be able to make use of a properly functioning website. In the new e-privacy regulation, the placing of cookies will only be permitted in the following cases:

- ▶ When only functional cookies are used;
- ▶ When the analytical cookies are only applied for personal use and never shared with other parties. Do you use Google Analytics? Then make sure that you work according to the new conditions;
- ▶ The internet user must, of course, have given their consent for the collection of data via the browser settings and this consent must be retractable as easily as it was given.

But what exactly is the difference between functional cookies and analytical cookies?

Functional cookies

Functional cookies are not subject to the Cookie Act and do not require the consent of the website visitor. The term 'functional' is used to indicate that the cookies must play a functional role on your site or service. Functional cookies could be about products in a shopping cart or remembering login details after selecting 'Remember login'.

Analytical cookies

Statistical programmes such as Google Analytics make use of analytical cookies in order to track the surfing behaviour of your website visitor. On this basis you can easily carry out targeted (marketing) actions on your target group by, for example, showing exactly those products that were indicated by the visitor's surfing behaviour. Through this data, websites are optimised and you can improve the user experience of your visitors. For these cookies you don't need permission either. However, visitors of your website must be made aware of this via a cookie or privacy statement.

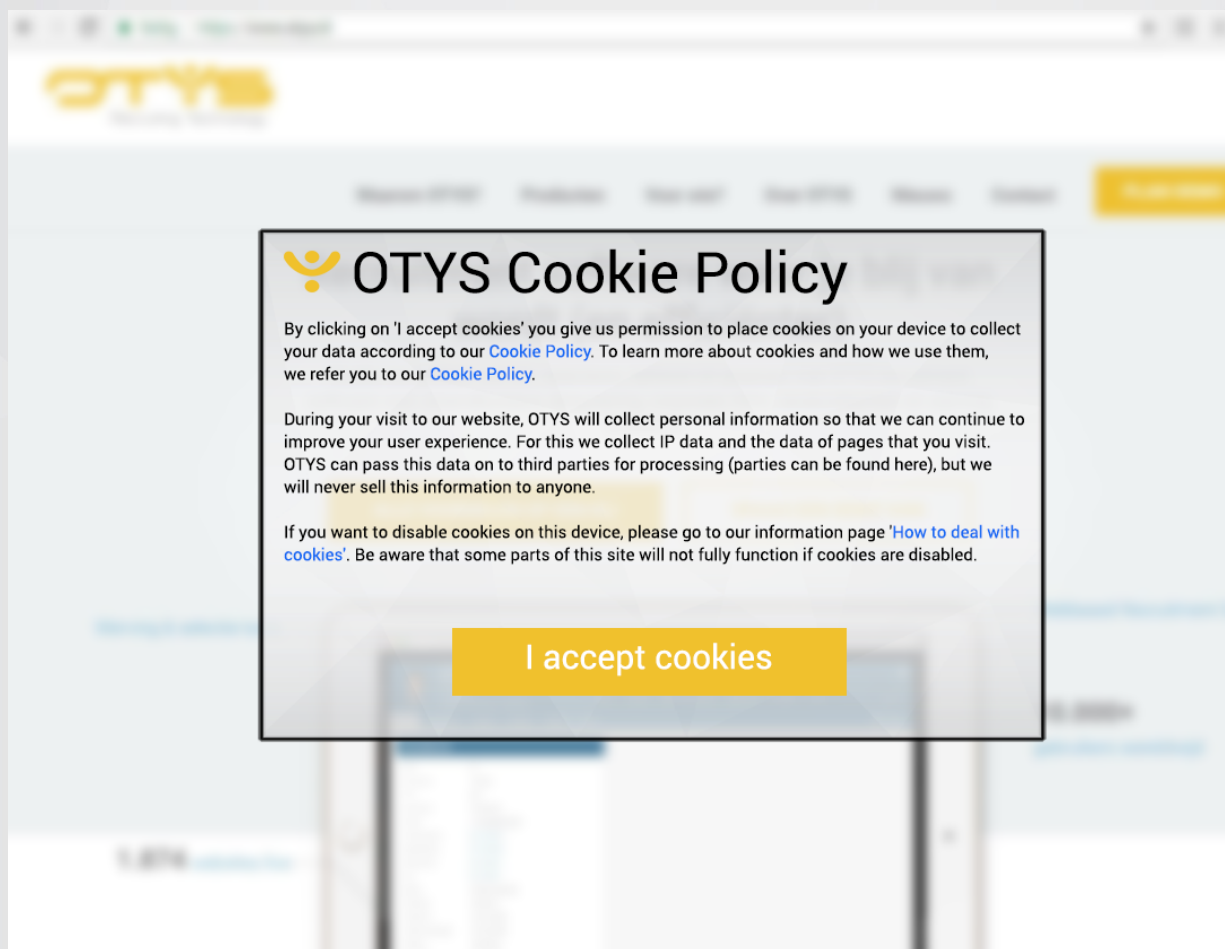
Cookie wall

According to the European Commission, gaining access to a website is 'essential for communication and participation in the digital economy'. Once the GDPR has come into effect, you will no longer meet the permission requirement by merely placing a cookie wall on your website, simply because you only inform the visitor about the cookies and not give them the option of giving their consent for the collection of data.

Access to data

That a visitor of your website must be able to access and review their data, and to have it changed or deleted at their request, also applies to cookies.

An example of a cookie opt-in can be found on the next page:



Documentation obligation



Documentation obligation

How can I keep a data register and what do I need to do this?

Under the GDPR, keeping a data register is mandatory for processors of personal data. You can assume that, in this day and age, every company processes personal data (e.g. if only for the purpose of personnel registers). The register of processing activities (data register) contains information about the personal data that you, as controller (OTYS customer), process. How you set up this register is up to you. The GDPR does, however, prescribe the type of information that should be shown in the register. You must also be able to immediately show the register if the Dutch Data Protection Authority requests this.

Content data register

The regulation prescribes that controllers must include the following information in the data register:

- ▶ The name and contact details of:
 - *your organisation, or the representative of your organisation; - any other organisations with whom you have jointly established the purposes and means of processing;*
 - *the Data Protection Officer if you have appointed one;*
 - *any other international organisations with whom you share personal data.*
- ▶ The purposes for which you process the personal data. For example, for the recruitment and selection of personnel, the delivery of products or direct marketing;
- ▶ A description of the categories of persons whose data you process. Benefits recipients, for example, customers or patients;
- ▶ A description of the personal data categories. Such as the citizen service number (BSN), name and address details, telephone numbers, camera images or IP addresses;
- ▶ The date on which you have to delete the data (if this is known);
- ▶ The categories of recipients to whom you provide personal data;
- ▶ Do you share the data with a country or international organisation outside the EU? If so, you must indicate this in the register;
- ▶ A general description of the technical and organisational measures you have taken to secure the personal data that you process.

Deleted data does not need to be documented. In short, it must be stated per category what the purpose of the processing is, which retention period

is applied, etc. This must be done per category and not per individual.

As controller, OTYS has the obligation to set up a data register for itself. We are not responsible for the data registers of our customers. We could, however, facilitate this and have, therefore, made a template available in which this information can be easily kept in an organised manner. This template can be downloaded from our website <https://www.otys.nl/dataregister.html>

Accountability



Accountability

How can I prove to the Dutch Data Protection Authority that I have obtained consent?

Online consent

In the event of an online request for the consent of persons where the processing of their personal data is concerned, the information regarding the visit to the website in which they gave their consent can be recorded. This information can be combined with:

- ▶ Documentation about the process in which you have laid down the way you receive and record consent (e.g. the overview in chapter 'Processes OTYS' in which the complete processes of OTYS are described - provided that these processes are followed, of course).
- ▶ A copy of the information that data subjects have received prior to the consent given (in OTYS this could be the vacancy to which the candidate is linked).

It is deemed insufficient to show valid consent by only referring to the automatic registration of consent by the website. The information that has been provided to those involved is then missing.

OTYS automatically records the type of interaction form (if a candidate is automatically created), at what time this took place and via which IP address the candidate was created.

If use is made of other processes (manual entry), the information regarding the origin is not automatically added to the candidate details. In this case, the confirmation email must be added to the file.

Right of access



Right of access

What does the right of access entail?

People have the right to access their personal data. This means that they can ask an organisation whether it has recorded their personal data and if so, what data. They do not have to provide a reason for an access request.

If someone requests access, the organisation must let them know in a clear and understandable way:

- ▶ Whether the organisation uses their personal data, and if so:
- ▶ Which data it concerns;
- ▶ For what purpose it is used;
- ▶ To whom the organisation may have forwarded the data;
- ▶ What the origin of the data is, if known.

If you followed the procedure well, all this information should be recorded in your data register.

Scope of the right of access

The right of access only concerns access to someone's own data. This means that people do not have the right to access information about others.

Does an organisation use personal work notes as a reminder? These notes do not fall under the right of access. What if the organisation subsequently saves this data to a file or provides these notes to others? In that case, the person concerned will also have the right to access these notes.

Introduction reports to customers

If the introduction report is purely intended for exchanging ideas and is only used internally, the right of access does not apply. Notes in an introduction report only fall under the right of access if they are also part of the file. If the introduction report is used to present a candidate to another relationship (i.e. not internally), the candidate has the right to view the data.

In respect of viewing the data, the first time visitors ask to view the data it must be made available to them free of charge. For all subsequent viewing requests an organisation may charge an acceptable fee. In addition, requests may be rejected if the data is intended for improper use.

Visitors have the right to receive all data in a structured and understandable document

that they can share with third parties.

Data portability

The General Data Protection Regulation (GDPR) gives data subjects (those whose personal data is processed) more control where the processing of their data is concerned. It strengthens and expands their rights to privacy.

Under the GDPR, people are given the right to data portability, i.e. the transferability of personal data. This means that they have the right to receive the personal data that any organisation may have of them. In this way they could easily pass on their data to another supplier of the same type of service, for example.

In this respect OTYS facilitates the Print CV in which all necessary data is transferred. Right of access also has an effect on emails. OTYS currently does not (yet) facilitate an automated process for downloading.

Other privacy-related matters



Other privacy-related matters

Not part of the GDPR but very important to be aware of!

Camera surveillance on the shop floor

Using camera images can be an efficient way to prevent theft or fraud. For this reason, it is permitted to use cameras on the shop floor. However, there are a number of conditions that must be met. You must have a legitimate interest in installing cameras and camera surveillance must be necessary. This means that there is no other option to reach the goal that is being pursued and thus cameras are used. The images may not contain sound because this is not necessary for the purpose. Filming intimate places, such as the toilet area, is absolutely forbidden. Informing people orally of camera surveillance is not considered sufficient as it cannot be determined who has or has not been informed of this surveillance. Display signs, for example, that indicate the use of camera images.

Posting photos of employees or other persons on social media

Photos and videos in which persons are recognisable are considered personal data. Therefore, you need that person's consent to place such photos. Under the GDPR you will soon have to prove that the consent you have obtained for the publication of the visual material is valid. In addition, the possibility of withdrawing consent must be as easy as giving it.

Afterword OTYS



Afterword OTYS

Currently, there are many existing functionalities in OTYS that help our customers in being compliant. Even when it comes to the GDPR. However, through the process of continuous development OTYS wants to make these functionalities even more convenient and user-friendly.

Examples of relevant functionalities are:

- ▶ The deletion of candidates and files;
- ▶ A consent email after you have added a candidate to your database via the LinkedIn manager;
- ▶ A notification when the 4 weeks after the application process has been completed are up;
- ▶ An automated consent email after 12 months;
- ▶ The complete deletion of files.

OTYS has already started work on the above functionalities and will provide updates once changes have come into effect. You can also expect several videos from OTYS in January, which will show, step by step, what OTYS facilitates and what you will still have to do yourself.

The flexibility of OTYS

That the OTYS platform belongs to everyone is what has made our platform so innovative over the years. This also means that our customers can change an infinite number of settings themselves, including the settings that ensure your compliance. As OTYS, we do not want to change this because we believe that we have to facilitate the compliance of our customers. What we don't want to do is force them to be compliant, whether they want to or not. Every customer is different and if they want to apply a retention period of 6 months instead of 12 months, we must be able to facilitate this. Hence continuous flexibility. However, all functionalities will be set, by default, in accordance with the GDPR.

ISO certification

OTYS does everything in its power to operate in accordance with legislation and this also where security is concerned. This means, among other things, that an annual SOC2 audit is conducted and that we make the report available to our customers. In addition, we store our data via our partner Sentia, who is ISO27001 and ISAE 3402 TYPE II certified.

As the authorities do not ask for an ISO27001 certificate, this is definitely not a requirement. SOC2 is a good alternative for ISO27001 and also more aimed at IT businesses.

Processes OTYS

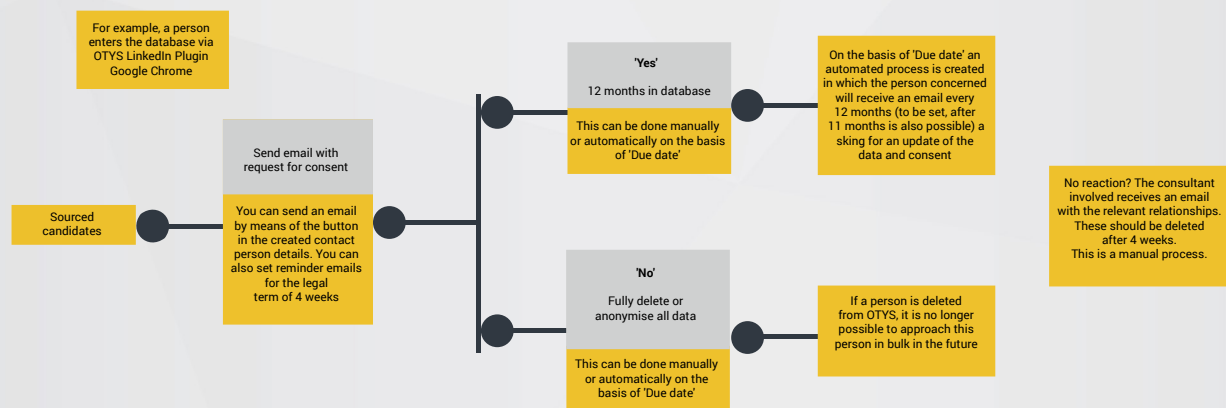


Which processes do we distinguish?

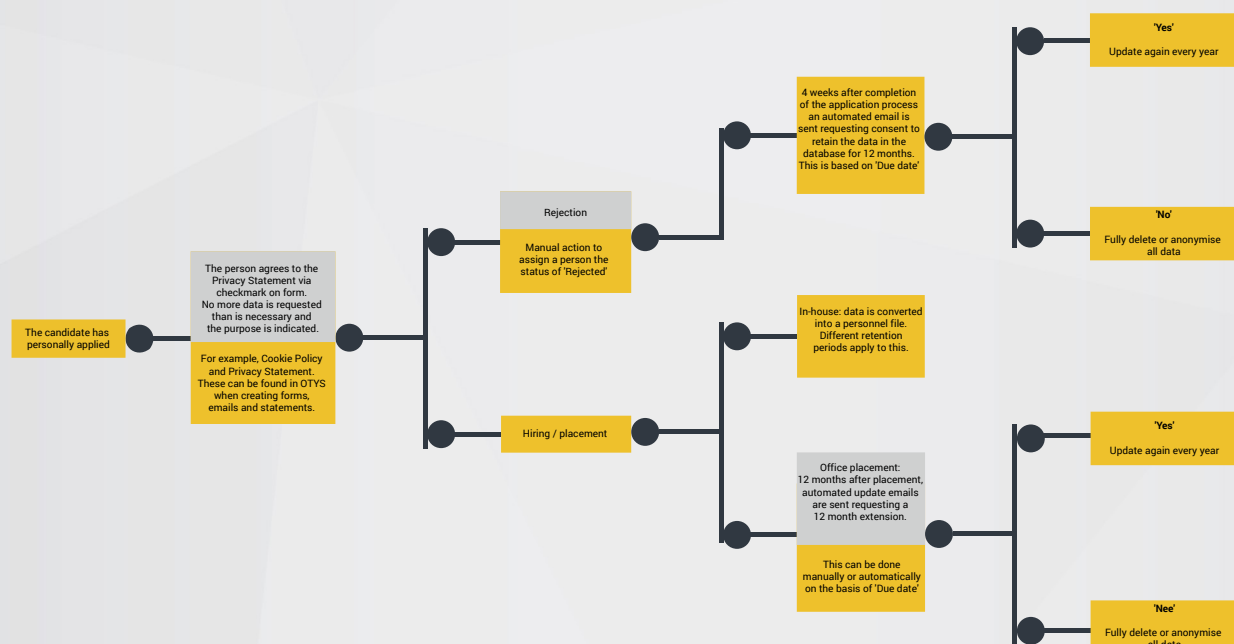
What is required according to the GDPR and what does OTYS do to accommodate this?

As a user of OTYS there are plenty of options to ensure your compliance. At OTYS we have been able to distinguish a number of processes and it could be relevant for our customers to know how we have organised these processes under the GDPR. We have presented these processes in well-arranged diagrams that clearly show what is needed according to the legislation and also how OTYS deals with this.

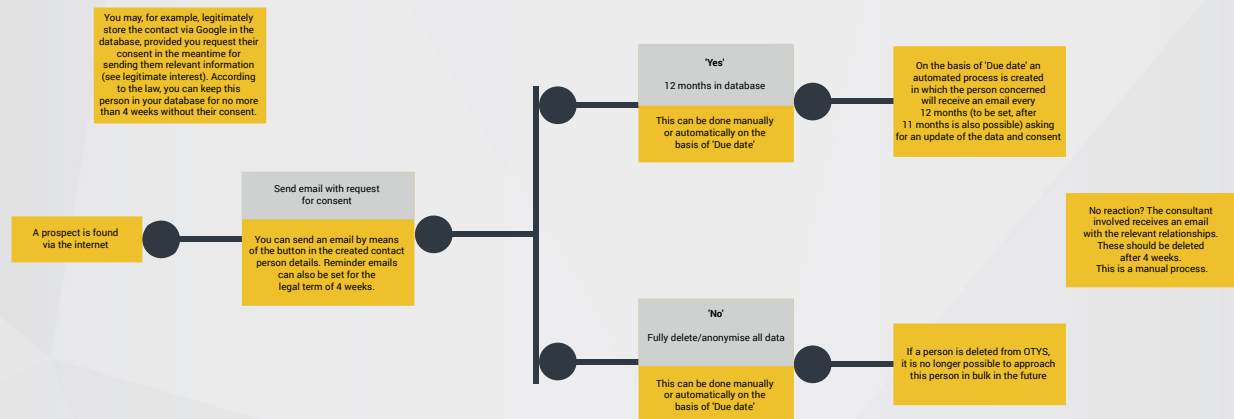
Process 1 - Sourcing



Process 2 - Application



Process 3 - Prospect (relationship)



Process 4 - Newsletter (marketing)

