WARDYŃSKI & PARTNERS

Outsourcing in practice

Warsaw, March 2016

Contents

Why outsourcing?

Danuta Pajewska, Paweł Mazur

Outsourcing continues to be an appealing solution for businesses. But for it to generate benefits rather than legal problems, a number of issues must be analysed—from the liability rules governing the parties to issues of state aid and data protection.

The concept behind outsourcing is to rationalise costs by drawing on the services and resources of specialised external firms. By outsourcing, businesses benefit from the knowledge and experience of professionals in the given area without having to invest in an in-house unit. It is easy to find an external contractor that will execute less-complex tasks, usually technical and repetitive, without having to create dedicated in-house positions and a system for managing them. And in capital groups, companies sometimes needlessly duplicate the same tasks, which ends up being more expensive than if these tasks were performed by one unit, either external or internal.

The tasks companies outsource most often are associated with IT systems and HR management (e.g. recruitment, payroll, training, and personnel records), sales and marketing, customer service (call centre), accounting and administration (bookkeeping, invoicing and purchasing), and logistics (e.g. transport, distribution, warehousing and order completion).

The outsourcing services market is one of the fastest-growing sectors of the Polish economy. An estimated over 560 centres employ about 170,000 people and the forecast for the end of the year is for an increase in employment by another 10,000–20,000. Investors choose Poland as a location for services due to the proximity of potential customers in Western Europe, a large supply of skilled personnel with a particularly good knowledge of foreign languages, relatively low labour costs, and good modern infrastructure. Kraków was recognised in the Tholons Top 100 Outsourcing Destinations 2016 report as the best European city for outsourcing services and 9th globally, and two other Polish cities—Warsaw (25th) and Wrocław (58th)—were among the world's top 5 movers. Kraków accounts for about 25% of the market for modern business services in Poland, with about 40,000 people employed there in that sector.

Outsourcing agreement

When planning and performing outsourcing, it is crucial to clearly specify the purpose of the outsourcing, provide an analysis of the involved costs, benefits and risks, determine the exact extent of outsourced tasks, and ensure that the terms of the contract with the external service provider are properly structured.

The contract should guarantee the outsourcer's right to oversee the execution and outcome of outsourced work, contain provisions for protection of data and personal information as well as clear rules for the use of the outsourcer's premises and equipment by the business performing the outsourced tasks, and clearly define the terms and procedures of contract termination. Liability issues are equally important, as they govern the corpo-

rate responsibility of the outsourcer's management board for contracting out the tasks.

The scope of liability of the service provider is governed by the terms of the contract and is only constrained by rules of civil law prohibiting an exclusion of liability for intentional injury. In other respects the parties to the contract can freely determine the scope of liability for non-performance or improper performance of services, and possibly provide for contractual penalties so long as they are reasonable. The amount of a contractual penalty is not tied to the actual amount of the loss, but if the outsourcer wants to ensure the right to seek damages in excess of the contractual penalty this must be stated in the contract.

When outsourcing services are governed by specific laws and overseen by an industry regulator, both sides to the outsourcing contract must ensure absolute compliance with the applicable regulations.

Selection of service provider

A series of regulations opening up access to certain professions have recently come into force. This means, on the one hand, that the supply of specialised services will increase, but, on the other, it creates the need to exercise particular diligence when selecting an outside contractor, as an incorrect choice may entail negative consequences for the outsourcing company and members of its governing bodies. The risks of outsourcing primarily involve the risk of harm to reputation and the connected risk of losing customers, as well as the risk of civil and criminal liability of the company and the members of its management board. Contracting out certain tasks does not mean that the liability for performing them is shifted to the contractor. On the contrary, it makes it necessary to manage the risk of liability to customers or employees for actions by the outside third party.

When outsourcing accounting services it should be kept in mind that the manager of the in-house unit overseeing these services remains responsible for the execution of accounting tasks also when they have been entrusted to an outside contractor. If the unit is managed by a group of people and there is no single individual bearing overall responsibility, then that responsibility is shared by all group members.

It is important to specify in the outsourcing contract the scope of entrusted tasks and the related rights and obligations of both parties. This can be vital for determining whether the contractor's obligation is to make its best efforts or to achieve a particular result. If the services are of poor quality, this poses a risk also for the outsourcer, as in most cases it will not be a defence that it contracted the services out to a third party. Therefore, the outsourcer should secure for itself in the contract the right to continual supervision of the performance of the outsourced services and the right to receive real-time information on the progress of performance. Depending on the nature of the services, it should establish a contingency plan in case the contractor runs into difficulties in delivering the services. It is also necessary to decide in the contract whether the service provider may subcontract the performance of the services, and if so, under what conditions and on whose responsibility.

Data protection

The Personal Data Protection Act provides for criminal sanctions for unauthorised release of personal data, failure to adequately protect personal data, or non-registration of personal data processed by the data controller. In addition to criminal liability, there is

also a risk of civil liability for personal losses. It is therefore necessary to determine to what extent the external contractor will have access to legally protected information concerning customers and to ensure that this information is properly protected. The outsourcing contract should expressly state that personal data has been entrusted for processing only to the extent specified in the contract and obligate the external contractor to meet the organisational and technical requirements provided for data controllers. The outsourcer is responsible for data processing performed by external contractors.

Adequate protection of classified data such as corporate or professional secrets and other confidential information must also be ensured. If the performance of outsourced services necessitates transferring this type of data, it should be done cautiously, to the extent justified by the type of outsourced services, and providing the outsourcer the ability to inspect the classified-data protection system. (For more on data protection aspects of outsourcing, see also the articles "New era for personal data protection" and "Transfer of personal data to the United States: Privacy Shield v Safe Harbour.")

State aid

Companies intending to establish an outsourcing hub may be interested in related financial incentives, particularly those based on location. Investors should consider the benefits of setting up business in a special economic zone, taking advantage of assistance programmes, obtaining reimbursement for the costs of equipping work stations or providing training, and accessing direct aid.

Doing business in a special economic zone under a licence provides the opportunity for exemption from corporate income tax. However, it should be noted that licences are not granted to businesses engaged in regulated activities (particularly financial institutions).

Poland is one of the largest beneficiaries of EU funds in 2014–2020. These funds are distributed to businesses through assistance programmes. The assistance may be allocated to various business projects. Businesses can apply for assistance through competitions organised by the implementing institutions and receive the funds under an agreement signed with the institution.

Reimbursement of the costs of equipping work stations is available if the employer meets certain criteria, for example hiring people registered as unemployed, submitting an application to the local authorities and signing an agreement with the municipality. The beneficiary is required to maintain employment at subsidised positions for a specified period.

It is possible to receive a partial refund of training costs (up to 80% but not more than three times the average monthly wage) on the basis of a training proposal submitted to the county administrator, after conclusion of the relevant agreement. The subsidy does not usually exceed 50% of the training costs.

Obtaining direct aid is possible on the basis of a proposal adopted individually for a specific project by the Council of Ministers for investment and employment costs. Direct aid is granted following negotiations which are not restricted in scope or duration, concluding in signing of the relevant agreement. Such aid must be notified to the European Commission.

Outsourcing no escape from liability for telemarketing without consent

Rafał Kuchta

The Supreme Court of Poland ruled on 17 February 2016 that an entity conducting direct marketing using automated generating systems (in that case SMS ads) is liable for failure to obtain consent from recipients also when it has contracted out the marketing to an external firm.

The case involved a marketing campaign by a telecom operator which sent text messages to its subscribers in 2010–2011 encouraging them to participate in a promotional lottery. Poland's telecom regulator, the president of the Office of Electronic Communications (UKE), fined the operator PLN 5 million for conducting direct marketing using automated generating systems without the consent of the recipients.

The fine was imposed pursuant to Art. 209(1)(25) of the Telecommunications Law of 16 July 2004, under which any person (and therefore not just a telecom company) who does not comply with the obligation to obtain the consent of the subscriber or end user pursuant to Art. 172 of the Telecommunications Law is subject to a fine. Under Art. 172(1), use of automated generating systems (and from the end of 2014 also end-user telecommunications devices) for direct marketing purposes requires the prior consent of the subscriber or end user.

In other words, simply put, conducting marketing campaigns addressed to specific persons by telephone (e.g. SMS) or computer (e.g. e-mailing) requires the user's consent before sending the person ads or offers. It should be stressed that under the Telecommunications Law, such consent cannot be implied or presumed from some other statement (for example concluding a contract to use the services of the advertised firm). Such consent may be given by electronic means (on condition that it is recorded and is confirmed by the user), but the user must have the option of withdrawing consent at any time, easily and without any fees.

In this case, the regulator found that the telecom operator had violated these regulations because it did not obtain any consent from the recipients of the marketing, and this justified imposition of the fine. The telecom did not agree with the decision and challenged it in court. The telecom argued in its defence that it was not liable for failure to obtain the users' consent because it had hired an outside firm to conduct the marketing, and therefore it was the contractor that should be liable for any violations.

Because of doubts raised by this issue, the appellate court submitted a legal question to the Supreme Court, which by resolution dated 17 February 2016 (Case III SZP 7/15) ruled that a fine based on these regulations may also be imposed on a telecom which has "contracted with another entity using automated generating systems for the purpose of

direct marketing of the services of the telecom among its subscribers or end users, using a supplied database of telephone numbers."

This ruling appears to be universal and essentially applies to any entity contracting out telemarketing to another firm, particularly considering that in the oral justification for the ruling delivered by the court, as reported at the UKE website, the Supreme Court stressed that the prohibition under Art. 172(1) of the Telecommunications Law is broadly applicable in terms of the entities it covers. Moreover, it should be assumed that this liability applies also to outsourcing of marketing via end users' telecommunications devices (a broad category covering most devices connected to a telecommunications network, such as computers and phones). The dispute in which the Supreme Court issued its resolution arose under the prior law, but the only change since then in Art. 172(1) of the Telecommunications Law consisted in adding to this provision the words "end-user telecommunications devices." Thus the holding by the court is universal in nature. It does not appear that liability in this case depended on the specific technical means used for the marketing.

However, one should be cautious in concluding that in the case of outsourcing of marketing to a third party, liability for failure to obtain the required consent will always be borne by the party contracting out this service. The ruling by the Supreme Court was issued under a specific set of facts, and it also appears from the oral grounds for the ruling that in this case the contractor conducting the marketing used a database of recipients provided by the other party and was not authorised to verify the database. It cannot be ruled out that if the telecom had imposed more extensive obligations on the contractor with respect to preparation of the marketing campaign, e.g. a duty to obtain the consent of the recipients, then it would nonetheless be the contractor that would be liable for any irregularities. But for now it is difficult to evaluate the significance of the Supreme Court resolution for direct marketers. The written justification for the ruling, which should be published in the near future, will no doubt be highly instructive.

New era for personal data protection

Sylwia Paszek, Agnieszka Szydlik, Katarzyna Żukowska

Work is underway on a General Data Protection Regulation for the EU. The changes expected in the new legislation will be important for outsourcing companies. Among the planned changes, there will be severe sanctions for violation of data protection regulations.

On 17 December 2015, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs voted in favour of the proposed Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of per-

sonal data and on the free movement of such data. The draft adopted is the result of several years of legislative work, discussions among stakeholders, and weighing of competing priorities. The proposal is a point of departure for further legislative work and may undergo further modifications. Nonetheless, it gives a clear picture of the General Data Protection Regulation which is soon expected to become law. A major reform of the data protection system throughout the European Union is about to take place.

When enacted, the General Data Protection Regulation, as it is known, will apply directly in the member states of the European Union, superseding the Data Protection Directive (95/46/EC) and its implementations in national law (in Poland, the Personal Data Protection Act of 29 August 1997).

In this article we highlight selected changes to be introduced when the General Data Protection Regulation is adopted and enters into force which may be particularly important for the outsourcing sector.

Scope of application of the regulation

The regulation is to apply to processing of personal data when the processing occurs in the context of the activity of a data controller or data processor based in the EU, regardless of whether the processing occurs in the EU. This means that it will be necessary in each case to analyse the factual circumstances under which the controller processes data.

The regulation will also apply to processing of data of entities from the EU by a data controller or processor based outside the EU, if the processing is connected with offering of goods or services (including free of charge) or observation (monitoring) of the behaviour of data subjects, if the monitoring occurs in the EU.

The regulation contains a number of new solutions designed to make it easier to conduct business operations in compliance with data processing rules. These include:

- **Application of a single regulation in all EU countries**—the same legal and business solutions may be applied across numerous jurisdictions
- **One-stop–shop rule**, under which a business will be subject to oversight by only one national data protection authority, even if it operates in numerous EU countries
- **Risk-based approach**, which can moderate the obligations of a data controller depending on the actual risk to data protection presented by the data controller's operations.

Data controllers and processors

The draft regulation addresses the requirements for entities processing data more specifically than the current law. For example, the controller is required to select an entity providing adequate guarantees of implementation of appropriate means and technical and organisational procedures so that processing of the data meets the requirements of the regulation. It also specifies the elements that must be established in the agreement between the data controller and the data processor.

Notification of data protection breaches

The draft regulation imposes on data controllers an obligation that does not exist under current law to notify the supervisory authority (in Poland, the Inspector General for Personal Data Protection—GIODO) of a breach of personal data protection. The notification must be made without undue delay, but no later than 72 hours after the event. If this deadline is not met, the reasons for the delay

must be explained. The notification must include, at least, a description of the nature of the breach, including the categories and number of data subjects potentially affected, the identity and contact details of the data protection officer or other contact point where more information can be obtained, the anticipated consequences of the breach, and the measures proposed or taken to minimise or eliminate the negative consequences of the breach. If complete information cannot be provided immediately, it should be supplemented when possible, along with documentation of remedial measures so that the supervisory authority can verify that they are proper and adequate. Data processors will be subject to a similar notification obligation in the case of a breach, but they should notify the data controller.

The data controller also has to notify the data subject of a breach of data protection, providing an understandable description of the breach, the potential consequences, and the remedial measures. This notice will be required only when the breach carries a high risk of infringement of the rights and freedoms of the data subject. The data controller will be released from the requirement to notify data subjects if it has implemented technological and organisational measures to protect the data affected by the breach, particularly by rendering the data unintelligible to third parties (e.g. through encryption), where the measures taken by the controller have eliminated the risks to the rights and freedoms of the data subjects, and where the notification of data subjects would be disproportionately burdensome to the contractor (in which case the direct notification of data subjects can be replaced by public announcements or other means with similar effect).

The obligation to report data breaches is a major change from current law. Now data controllers and processors do not have to disclose such events. Outside of the public eye, they make their own choice of remedial measures according to their capabilities. Any inadequacies or incompleteness in the solutions they adopt may only be identified in the event of an inspection by GIODO. The proposed model will ensure that in the event of a breach, the data controller will implement remedial measures in close dialogue with GIODO and under GIODO's supervision. This will reduce the risk that measures will be used that are not adequate to the nature of the breach.

Sanctions for violating data protection regulations

The current law in Poland provides sanctions for violation of data protection regulations (for petty offences and criminal offences), but their application is typically limited to liability for a petty offence (not very severe), while it is exceedingly rare for criminal responsibility to be imposed (because the societal harm of the act is deemed to be low). Thus there is an absence of a proportionally severe sanction to be applied even in the case of small-scale violations.

This gap will be filled by administrative fines imposed by GIODO. The amount of the fines would reflect such factors as the nature, gravity, duration and consequences of the violation, the degree of fault, the infringer's responsibility for implementing proper technical and organisational measures, the remedial actions taken to limit or eliminate the negative consequences of the violation and cooperation with GIODO in this respect, previous violations, and the manner in which GIODO learned of the violation.

The maximum fine, depending on the nature of the violation, would be EUR 10 million or 20 million, or in the case of an enterprise, 2% or 4% of its total annual revenue in the preceding year. The member states are to adopt executive regulations concerning inspection proceedings and procedures for imposing and enforcing penalties, which should be proportionate but severe enough to act as a deterrent.

Data controllers and processors would also be liable (based on fault) for injury caused by unlawful processing of data. Any person who suffers material or non-material damage as a result of unlawful processing of personal data may demand compensation. The data controller's liability is limited to cases where it has violated the regulation, while the data processor's liability is limited to violation of the provisions of the regulation addressed specifically to data processors or for acting contrary to the data controller's instructions. The controller and the processor would bear joint and several liability for the same occurrence, but could assert claims for recourse between one another.

Transfer of personal data to the United States: Privacy Shield v Safe Harbour

Sylwia Paszek

Invalidation of the Safe Harbour decision created a gap in the system for transfer of data from Europe to the US. The question arose of how to evaluate the legality of existing data transfer practices based on Safe Harbour, and what rules to apply in the resulting vacuum.

On 6 October 2015 the Court of Justice of the European Union ruled that registration by American companies obtaining personal data under the Safe Harbour system is not sufficient grounds for transferring personal data from the EU to the US. The court held that the requirements of that programme did not ensure an adequate level of data protection, and therefore more restrictive security measures than those provided by Safe Harbour are required.

Doubts as to the adequacy of Safe Harbour had been building for years, and mostly resulted from the absence of a mechanism for involving the US administrative and judicial system in guaranteeing and enforcing data protection, as well as the practically unlimited possibility of subcontracting the processing of personal data to entities operating outside of the Safe Harbour system.

The operational paralysis following invalidation of Safe Harbour required the involvement of stakeholders as well as measures to restore trust in the transatlantic flow of data after reports of surveillance from 2013, and development of new rules.

When the European and American sides began working on filling the gap left by Safe Harbour, the parties had already reached an "umbrella agreement" (the European Commission announcement on completion of the negotiations begun in 2011 was published on 8 September 2015). It establishes at a high degree of generality the legal framework for cooperation between the parties in protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences, including terrorism. The umbrella agreement includes such mechanisms of protection as:

- Limitation of data processing to clearly defined purposes
- Obligation to obtain consent of the national data protection authority of the country originally providing the data in the case of onward transfer of data beyond the EU or US
- Prohibition of retaining data beyond the period needed for processing of the data
- Right of data subjects to access and rectify their data
- Duty to notify breaches of data protection rules
- Right of data subjects to pursue claims arising out of data violations in the country where the violation occurred (within the EU or the US).

As indicated, the umbrella agreement has very limited application, as it is generally addressed only to law enforcement authorities. Thus it replaces Safe Harbour only to a small degree. But it cannot be ignored that the agreement provides for a system of enforcement of data protection rights that did not exist before in relations between the EU and the US, and also recognises the primary of European principles.

Then, on 29 February 2016, the European Commission announced that together with the US Department of Commerce it had completed negotiations of the rules for transatlantic exchange of personal data for commercial purposes, i.e. *de facto* it had completed work on a mechanism to replace Safe Harbour.

The negotiations resulted in publication of a draft adequacy decision—Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield.

Both the draft decision and the texts implementing the rules for safe transfer of data include rules for data transfer which must be observed by businesses, as well as written assurances by the US government concerning enforcement of the arrangements, including guarantees and limitations on access to data by public authorities.

The Commission confirms that the level of data protection after adoption of the rules will be adequate: the guarantees in force in the case of the flow of data between the EU and the US under the new rules will be the same as the standards for data protection within the EU. This will be achieved through:

- Strong obligations on companies and robust enforcement
- Tighter conditions for onward transfer of data by businesses participating in the programme
- Ensuring transparency in access to personal data by the US government, including enabling Europeans to pursue claims against American intelligence services

- Implementation of several mechanisms for redress of claims (including a fixed deadline for companies to respond to complaints, arbitration and other forms of ADR)
- Annual joint review mechanism under which the parties will monitor the functioning of the rules for safe transfer of data and other issues.

It will still be some time before the final version of the decision is issued and it enters into force. On the EU side the draft decision must be approved by representatives of the member states and presented to the Article 29 Working Party (composed of the EU's national data protection authorities) for an opinion. The American side must prepare the procedures and instruments necessary to ensure the enforceability of the Privacy Shield programme.

Reductions in employment in joint ventures by competitors

Dr Szymon Kubiak

In today's knowledge-based economy, consolidations of enterprises are common—sometimes even between competitors. Employment reductions are a natural part of any consolidation, but are a source of legal risks for merging competitors. Such risks are hard to eliminate, but does it have to end in stalemate?

Imagine a joint venture planned between enterprises that have so far been competitors. In numerous jurisdictions, including Poland, each company plans to consolidate its main line of business with similar activity conducted by a competing firm.

It may come as a surprise to many people to learn that in such a case, the most interesting and most problematic issues may not lie in the field of competition law, but in the field of employment law. This occurs particularly when at the level of the holding companies whose subsidiaries are creating the joint venture a global transaction framework agreement is entered into specifying such items as the maximum number of employees from each of the entities who can join the newly created joint entity in each country covered by the agreement. In the case of our hypothetical client, let us suppose that this number is smaller than the number of persons currently working at the Polish subsidiary. The fate of the rest of the workers is then pretty much sealed.

What is allowed before consolidation?

The hypothetical fact situation described raises a number of questions. The most important of them is whether such a global

agreement can effectively define the number of employees who will be "transferred" (whether automatically, i.e. under Polish law pursuant to Art. 23^1 of the Labour Code, or on the basis of offers of employment presented and accepted, which in practice results in dissolution of their employment relationship by agreement of the parties in connection with receiving an offer of employment from a new employer).

The answer to this question is generally negative. Pursuant to the established case law of Supreme Court of Poland under Labour Code Art. 23^1 and of the Court of Justice of the European Union under the Transfers of Undertakings Directive (2001/23/EC), contractual specification or modification of the number of employees subject, in this case, to transfer by operation of law to the newly established employer should be regarded as ineffective against the employees. In Poland, conducting layoffs of employees under these conditions will carry a high risk of violation of Labour Code Art. 23^1 §6, under which transfer of the workplace or part of the workplace cannot provide grounds justifying termination of employment by the employer.

Nonetheless, the business and operational purposes of the newly established joint venture typically require conclusion of an agreement structured in this way. This is because the optimal business operations of the newly established entity will require a certain number of people employed at specific positions, and not one person more.

Risk reflected in costs

So is there any room for manoeuvring? Certainly. One avenue to consider is termination of employment e.g. by agreement of the parties, ideally at the request of the employee (which typically requires additional financial incentives). Even that is not a risk-free approach, however (for reasons that go beyond the scope of this article).

The stated grounds for termination could be entirely unrelated to transfer of the workplace or part of the workplace, but if the employee appeals to the labour court it may be difficult indeed for the employer to defend these grounds.

Even lawyers with many years of practice can be surprised at their clients' willingness to accept a high level of risk in this respect. They treat the risk as entirely secondary to the business targets of the transaction. This clearly depicts the demands and realities of the contemporary economy.

Traps in selection of employees

The next question we must ask under these hypothetical facts is whether, prior to establishment of the joint-venture company, each of the existing employers can select which of its own employees will be laid off (including through group layoffs) based on specified "business and operational needs," that is, using criteria determined independently by each of the employers.

The answer is not obvious, and the problems only escalate. We should bear in mind that competing entities are involved, which means that difficulties in communicating should be expected, as well as a lack of trust and a disinclination or inability to share employment procedures (e.g. in terms of the employee evaluation systems applied by the employers). On top of that, the systems and criteria for employee evaluation applied in the past by each group may be entirely incompatible.

Lawyer and HR consultant

So the situation does seem to be heading toward stalemate. Even the most skilfully conducted process for establishing the criteria for selecting employees to move to the newly

created employer (which for the staff not chosen will mean *de facto* group layoffs) will be subject to a substantial risk of being found to be illusory, because the only authentic criterion would be the business and operational needs of the newly created company, not those of the existing employers.

Here an additional challenge arises for legal advisers involved in such transactions. They need to balance the risks that have been signalled with the proposal (if possible) of innovative and creative solutions enabling the client to implement its ultimate business model. Such measures often extend beyond the traditional understanding of legal advice and shade more into the field of HR consulting. But lawyers handling employment matters must have this knowhow in order to meet the demands of today's clients.

So what options are there? Either conducting layoffs before establishment of the joint-venture company, but based on uniform and consistent selection criteria established by all of the employers, or conducting such layoffs after creation of the new employer (the longer after it is created the better), only after all of the staff of the existing employers become employees of the new company. The latter solution is optimal in terms of the ability to make an objective comparison of the usefulness of the employees for the company that is now in operation, considering the synergies as well as any problems connected with combining several groups of staff in a new entity.

Permissible external support

It should be borne in mind here that an employer conducting layoffs for economic reasons (not attributable to the employees), and thus for example in the case of a merger of the operations of companies through creation of a joint-venture company, must be able to prove that it applied fair and objective criteria in selecting staff for layoffs and considered all employees affected by the reasons forcing it to terminate employment. If rules for proceeding are established, particularly criteria for selecting staff to be laid off, they should also be applied consistently to all employees. Any departures from the adopted rules require strong and persuasive justification.

Particularly interesting and helpful in this context is the judgment of the Supreme Court of Poland of 1 June 2012 (Case II PK 258/11) concerning the employer's right to establish criteria for selection of employees for termination in group layoffs.

This ruling was issued in a situation where, in connection with a planned reorganisation and consolidation of the sales departments of two companies, an evaluation of the competencies of the employees of the two companies was conducted for the purpose of selecting staff to be laid off. In the area analysed by the court, there were three sales reps working for each of the consolidating companies. The consolidation resulted in duplication of coverage of their regions, requiring a reduction in the number of sales reps accordingly. The evaluation programme was conducted by an outside firm, which prepared the methodology for assessment of the employees based on its own knowhow in this field. The external advisers decided to use an assessment centre approach.

The court permitted the employer to use as the sole criterion for selection of staff to be laid off an assessment of the employees' competencies that were relevant from the point of view of the employer, ignoring other criteria deemed less important, such as their previous career path, length of employment, professional experience or formal qualifications (education).

This means that an employer is entitled to establish criteria for selecting staff to be let go in group layoffs so that the employees possessing the characteristics (competencies, attitudes and skills) most desired by the employer under the new, post-consolidation circumstances are retained.

The court's positive assessment of the role of external firms in this process is hugely important in practice, particularly when it comes to external firms offering services such as assessment centre, enabling a comprehensive and objective evaluation of employees and selection of staff for layoffs in a manner that is uniform across both of the merging entities. Based on this ruling, an employer choosing staff to be laid off may rely if it wishes exclusively on an assessment by professional advisers specialising in evaluation of employees' competencies and capable of conducting an objective evaluation based on a developed methodology.

An additional advantage of this approach is the confidentiality offered by an outside service provider—essential when the new employer is being established by companies who are currently strong competitors on the same market. The employers involved would naturally expect the external advisers to sign a strongly worded non-disclosure agreement.

Practice will show whether the use of assessment centre services gains in popularity in such cases. As the reader may surmise, the considerations are not entirely theoretical.

Authors

Danuta Pajewska is a legal adviser and a partner in charge of the Capital Markets and Financial Institutions practices. She handles issues related to the law of securities, capital markets and financial institutions, capital market transactions, corporate governance and compliance, particularly in relation to publicly listed companies, and outsourcing issues.

E-mail: danuta.pajewska@wardynski.com.pl

Szymon Kubiak, PhD, is a legal adviser, a partner and a member of the Employment Law Practice. He handles individual and collective Polish and European labour law and outsourcing. He has long-term experience in employment restructuring, including outsourcing and group dismissals in complex and cross-border employee transfers (including transfers of enterprises and parts of enterprises) and provides ongoing advice on atypical and flexible forms of employment and employment of temporary workers.

E-mail: szymon.kubiak@wardynski.com.pl

Paweł Mazur is *an adwokat* and partner. He heads the firm's office in Kraków. He represents clients in judicial and arbitration proceedings, particularly concerning infrastructure and construction projects, real estate, transport, and post-transaction disputes. He is responsible for developing the firm's Aviation Law Practice and involved in the Outsourcing Practice.

E-mail: pawel.mazur@wardynski.com.pl

Sylwia Paszek is a legal adviser and a member of the Life Science Practice. She is also responsible for the e-commerce, protection of privacy and telecommunications areas in the New Technologies Practice and leads the firm's Insurance Practice. She practises pharmaceutical law, medical products law, and food law. She also deals with regulatory requirements for other consumer products concerning product quality, production, certification, labelling, market authorisation, sales and advertising, as well as administrative requirements for conducting business in specific industries.

E-mail: sylwia.paszek@wardynski.com.pl

Agnieszka Szydlik is an *adwokat* and a member of the M&A and Corporate Practice at Wardyński & Partners. She is also responsible for the privacy protection area in the New Technologies Practice. She provides legal support for corporate acquisitions and due diligence. She also has experience in matters involving ongoing legal advice for businesses as well as personal data protection.

E-mail: agnieszka.szydlik@wardynski.com.pl

Katarzyna Żukowska is an *adwokat* trainee and a member of the Employment Law and Personal Data Protection practices at Wardyński & Partners. She handles individual and collective labour law. Her experience includes restructuring of employment involving group layoffs, transfers of workplaces or parts of workplaces, as well as advice on hiring and termination, including dismissal of high-level staff and protected workers. She also advises on data processing from the standpoint of labour law and takes part in due diligence projects.

E-mail: katarzyna.zukowska@wardynski.com.pl

Rafał Kuchta is an *adwokat* trainee in the New Technologies Practice. His advises on payment services, crowdfunding, telecommunications law, data protection and e-commerce, particularly regulatory matters and related contracts.

E-mail: rafal.kuchta@wardynski.com.pl

Outsourcing Practice

We have significant experience handling legal issues related to outsourcing processes for banks and financial services companies, high tech, payment card companies, and producers of electronics and pharmaceuticals.

We advise outsourcing companies as well as users of outsourcing services (including "internal outsourcing" within a capital group).

Our services include:

- Assistance in HR planning and administration (hiring, firing and delegation of staff, job transfers, payroll, training and development, and maintenance of HR records)
- Proper legal structuring of the outsourcing process (e.g. offer inquiries and selection of contractors)
- Negotiating and drafting of outsourcing agreements for such areas as sales and marketing, customer service and call centre, accounting and administration, including maintaining accounting books, invoicing, receivables and payables, clearing of transactions involving payment cards and cheques, logistics—transport and distribution, warehousing and storage, and quality assurance
- Legal safeguards in relations between staff of the outsourcer and the outsourcing company (trade secrets, privileged or confidential information, and personal data)
- Legal safeguards with respect to liability of company authorities for outsourcing of corporate functions and operations
- Legal compliance with respect to use of outsourcing services, where outsourcing is regulated or in the case of outsourcing in a regulated industry
- Comprehensive advice on public aid for outsourcing facilities (including tax incentives and EU funding)
- Tax advisory on such issues as optimising the tax treatment of outsourcing centres, transfer pricing issues, and taxation of outsourcing services.

The firm is a member of ASPIRE, an association of IT and business process services companies in Poland.

About Wardyński & Partners

Wardyński & Partners was established in 1988. Drawing from the finest traditions of the legal profession in Poland, we focus on our clients' business needs, helping them find effective and practical solutions to their most difficult legal problems.

The firm is particularly noted among clients and competitors for its services in dispute resolution, M&A, intellectual property, real estate and title restitution.

The firm now has over 100 lawyers, providing legal services in Polish, English, French, German, Spanish, Russian, Czech and Korean. We have offices in Warsaw, Kraków, Poznań and Wrocław.

We advise clients in the following areas of practice: agridesk, aviation law, banking & finance, bankruptcy, business crime, business-to-business contracts, capital markets, competition law, compliance, corporate law, difficult receivables recovery, employment law, energy law, environmental law, EU law, financial institutions, healthcare, infrastructure, insurance, intellectual property, life science, litigation, mergers & acquisitions, new technologies, outsourcing, payment services, personal data protection, private client, private equity, public procurement, real estate and construction, reprivatisation, restructuring, retail and distribution, sports law, state aid, tax, and transport.

We share our knowledge and experience through our web portal for legal professionals and businesspeople (www.inprinciple.pl), the firm *Yearbook*, and the "Law and Practice" series. We are also the publishers of the first Polish-language legal app for mobile devices (Wardyński+), available as a free download at the App Store and Google Play.

www.wardynski.com.pl

www.inprinciple.pl

Wardyński+

Wardyński & Partners
Al. Ujazdowskie 10
00-478 Warsaw

Tel.: (+48) 22 437 82 00, 22 537 82 00
Fax: (+48) 22 437 82 01, 22 537 82 01

E-mail: warsaw@wardynski.com.pl