UNIVERSIDADE POLITÉCNICA DO INTERIOR (UPI)

FORNECIMENTO DE SERVIÇOS GERAIS DE CONSULTORIA EM MATÉRIA DE GESTÃO GERAL

Avaliação de impacto das operações de tratamento de dados a que se refere o art.º 35º do RGPD – Regulamento Geral de Proteção de Dados

EXEMPLO DE CADERNO DE ENCARGOS

Cláusula 1.ª

Objeto

O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto principal a aquisição pela Universidade Politécnica do Interior (UPI) de serviços gerais especializados de consultoria em matéria de gestão geral para avaliação de impacto das operações de tratamento de dados a que se refere o artº 35º do Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679), doravante RGPD, de acordo com as especificações técnicas previstas no Anexo I ao presente Caderno de Encargos, que dele faz parte integrante.

Cláusula 2.ª

Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra os seguintes elementos:
   a) (...)

Cláusula 3.ª

Prazo do Contrato

O contrato terá início na data da sua assinatura e será válido por 180 dias, em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do Contrato.

Cláusula 4.ª

Obrigações principais do prestador de serviços

1. Sem prejuízo de outras obrigações previstas na legislação aplicável ou no Caderno de Encargos, da celebração do contrato, decorrem para o prestador de serviços as obrigações constantes das Especificações Técnicas do presente Caderno de Encargos.
2. A título acessório, o prestador de serviços fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação do serviço, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 5.ª

Forma de Prestação do Serviço

Para acompanhamento da execução do contrato, o Prestador de Serviços fica obrigado a, sempre que solicitado, reunir nas instalações da UPI com os seus representantes.

Cláusula 6.ª

Tarefas da prestação do serviço

Os serviços objeto do contrato compreendem as seguintes fases:

a) Fase 1 – Caracterização do contexto organizacional;
b) Fase 2 – Análise da informação;
c) Fase 3 – Avaliação de conformidade;
d) Fase 4 – Recomendações.

Cláusula 7.ª

Prazo de Prestação do Serviço

1. O prestador de serviços obriga-se a concluir a execução do serviço, com todos os elementos referidos nas especificações técnicas, anexas ao presente Caderno de Encargos, de acordo com as seguintes fases e datas:
    a) Fase 1, no prazo de 71 dias;
    b) Fase 2, no prazo de 28 dias, podendo iniciar-se após o final da Fase 1;

c) Fase 3, no prazo de 14 dias, podendo iniciar-se após o final da Fase 2;

d) Fase 4, no prazo de 21 dias, podendo iniciar-se após o final da Fase 3.

2. Os prazos previstos no número anterior podem ser prorrogados por iniciativa da entidade adjudicante ou a requerimento do prestador de serviços, desde que devidamente fundamentado.

Cláusula 8.ª

Receção dos elementos a produzir pela prestação de serviços

1. A UPI monitorizará em contínuo a prestação do serviço, com vista a verificar se o mesmo reúne as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei. No caso de incumprimento dos requisitos, a UPI, comunicará o facto num prazo de 15 dias.
2. (...)

Cláusula 9.ª

Objeto do dever de sigilo

1. O Prestador de Serviços deve guardar sigilo, mesmo após o termo do contrato, sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à UPI, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. Exclui-se do dever de sigilo previsto, a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo prestador de serviços, ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 10.ª

Preço Contratual

1. Pela prestação de serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a UPI deve pagar ao prestador de serviços os valores indicados na proposta adjudicada, os quais não podem, porém, ultrapassar €74.950,00 (setenta e quatro mil, novecentos e cinquenta euros), acrescido de IVA à taxa legal em vigor, durante a vigência do contrato.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à UPI, incluindo as despesas de aquisição,

transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 11.ª

Condições de Pagamento

1. A quantia devida nos termos da cláusula anterior deve ser paga no final de cada Fase e em função do valor apresentado para cada uma delas.
2. (...)

Cláusula 12.ª

Resolução do contrato por parte do contraente público

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a UPI pode resolver o contrato, a título sancionatório, no caso de o prestador de serviços violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao prestador de serviços.

Cláusula 13.ª

Resolução do contrato por parte do prestador de serviços

1. Sem prejuízo de outras situações de grave violação das obrigações assumidas pelo contraente público especialmente previstas no contrato e independentemente do direito de indemnização, o cocontratante tem o direito de resolver o contrato nas seguintes situações:

   a) (...)

Cláusula 14.ª

Resolução de litígios – Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal (...), com expressa renúncia a qualquer outro.

Cláusula 15ª.

Legislação aplicável

O contrato é regulado pela legislação portuguesa.

ANEXO I

ESPECIFICAÇÕES TÉCNICAS

Com o presente contrato pretende-se realizar a avaliação de impacto das operações de tratamento de dados a que se refere o artº 35º do Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679), doravante RGPD. O principal produto esperado como resultado da prestação do serviço é um relatório técnico com o diagnóstico da situação atual e um conjunto de recomendações devidamente planeadas.

Capítulo I
Ações

A principal ação a desenvolver na execução deste contrato é a realização da Avaliação de Impacto de Privacidade, que permita à UPI identificar as medidas a implementar para garantia da conformidade com o novo RGPD.

Como resultado desta ação pretende-se atingir os seguintes objetivos:

a) Identificar o impacto do RGPD sobre os processos organizacionais e Sistemas de Informação da UPI;
b) Identificar o nível de cumprimento dos diferentes elementos afetados (tratamento de dados, ficheiros, sistemas, serviços, processos, normas, papéis, etc.), com respeito aos requisitos e exigências estabelecidos pelo RGPD;
c) Identificar os riscos a que se encontram expostos os tratamentos de dados relacionados com os diferentes processos organizacionais em que se decompõe a atividade da UPI, tendo em consideração os aspetos sectoriais específicos da sua missão e atribuições;
d) Definir orientações, transversais a toda a UPI, para o cumprimento dos novos requisitos introduzidas pelo RGPD, tendo em consideração os diferentes fatores (antecedentes, prioridades, nível de maturidade, recursos disponíveis, etc.);
e) Estabelecer os planos (a curto, médio e longo prazo) para o cumprimento dos requisitos do RGPD nas diferentes Unidades Orgânicas da UPI.

O âmbito da Avaliação de Impacto de Privacidade engloba todas as Unidades Orgânicas e Serviços da UPI, enumeradas na lista a seguir, e inclui as deslocações necessárias para a sua concretização (localidade do campus indicado entre parêntesis):

- Serviços da Reitoria (...)
- Serviços de Ação Social (...)
- Faculdade E (...)
- Faculdade C (...)
- Faculdade P (...)
- Faculdade M (...)
- Faculdade S (...)
- Faculdade H (...)
- Faculdade D (...)
- Faculdade G (...)

- Escola F (...)
- Unidade E (...)

Para um melhor enquadramento do âmbito são apresentados no Anexo II os organogramas das diferentes Unidades Orgânicas e Serviços da UPI.

Capítulo II
Plano de ação

A proposta deverá apresentar um plano de ação detalhado com as seguintes fases (as atividades apresentadas constituem apenas uma referência base, a detalhar na proposta):

Fase 1 – Caracterização do contexto organizacional

- Recolha de informação sobre as estruturas e processos organizacionais, áreas de negócios, interlocutores e tecnologias;
- Medidas já implantadas;
- Entrevistas presenciais.

Fase 2 – Análise da informação

- Análise e avaliação dos riscos a que se encontra exposto a UPI, transversalmente a todas as suas Unidades Orgânicas e Serviços;
- Identificação das obrigações do RGPD com maior risco de incumprimento, bem como aquelas cujo incumprimento ocasionaria um maior impacto na UPI, considerando a sua probabilidade de ocorrência, fatores económicos, fatores relacionados com a missão própria como Instituição de Ensino Superior e fatores reputacionais, entre outros.

Fase 3 – Avaliação de conformidade

- Avaliação do nível de cumprimento dos controlos do RGPD, nomeadamente:
    - Princípios relativos ao tratamento /Qualidade dos dados;
    - Consentimento;
    - Categorias especiais de dados;
    - Informação;
    - Confidencialidade;
    - Direitos de Acesso, Retificação, Cancelamento, Oposição, Eliminação, Limitação do tratamento e Portabilidade dos dados;
    - Comunicação dos dados;
    - Acesso a dados por conta de terceiros;
    - Registro de atividades de tratamento;
    - Transferências internacionais;

- Notificação de violações da segurança;
- Avaliação de impacto da privacidade;
- Segurança do tratamento;
- Modelo de governança.

Fase 4 – Recomendações.

- Definição da estratégia de adequação ao RGPD por parte da UPI, tendo em conta:
  - O nível de maturidade da UPI e os casos específicos identificados, bem como o modelo de implementação mais adequado;
  - A planificação mais adequada, i.e., com um critério de baixo risco e impacto;
  - Nível de maturidade que será possível atingir no cumprimento dos processos estabelecidos pelo RGPD, atendendo aos diferentes recursos e elementos disponíveis atualmente;
  - Limitações e impedimentos atuais existentes na UPI para implementar os diferentes processos do RGPD;
  - Momento em que será oportuno introduzir elementos adicionais (capacidades, processos e tecnologia), de forma a incrementar o nível de maturidade no cumprimento dos diferentes processos do RGPD;
  - Plano de ação com o objetivo de reduzir a distância existente entre a situação atual de cumprimento da UPI e o nível de cumprimento ideal dos requisitos e controlos aplicáveis à instituição, estabelecidos pelo Regulamento.

Capítulo III
Entregáveis

Como resultado das ações a desenvolver, é obrigação do adjudicatário fornecer à UPI a seguinte lista de entregáveis, sem prejuízo de documentação adicional que venha a ser considerada essencial após a realização da Fase 1:

Fase 1

- Plano de execução do projeto, a aprovar nas duas primeiras semanas;
- Relatório de caracterização do ambiente envolvente

Fase 2

- Relatório de análise e mapa de riscos

Fase 3

- Relatório técnico detalhado com grau de (in)cumprimento e não conformidades identificadas.
- Relatório para a gestão de topo

Fase 4

- Plano de recomendações e ações a desenvolver

Os documentos de gestão do projeto e respetivos formatos, nomeadamente atas de reuniões, atas de entrevistas e relatórios de progresso serão definidos na reunião de *kickoff*.

Capítulo IV
Normas e referenciais

A execução dos serviços deverá considerar os referenciais e normas relevantes na área, nomeadamente:

- CIS CRITICAL SECUTIRY CONTROLS
- ISO 27001
- ISO/IEC 27005
- ISO 27018
- ISO 31000
- PCI-DSS
- NIST
- COBIT

A execução dos serviços deverá ainda considerar a legislação relevante, nomeadamente:

- Regulamento (UE) 2016/679
- Pareceres do Grupo de Trabalho do Artigo 29º da Diretiva 95/46/CE (Comissão Proteção de Dados);
- Legislação Nacional sobre Proteção de Dados – Portugal;
- Legislação específica relacionada com a atividade de Instituições de Ensino Superior, nomeadamente a Lei n.º 62/2007 – Regime Jurídico das Instituições de Ensino Superior.

ANEXO II

ORGANIGRAMAS

(...)